Universidad Carlos III de Madrid

TESIS DOCTORAL

IMPACTO MEDIÁTICO Y POLÍTICO DEL ACTIVISMO HACKER EN LA SOCIEDAD RED. ESTUDIO DE CASO: WIKILEAKS

Autor: Alberto Quian
Director: Carlos Elías

Universidad
Carlos III de Madrid

TESIS DOCTORAL

Impacto mediático y político del activismo hacker en la sociedad red. Estudio de caso: WikiLeaks

Autor: Luis Alberto Pampín Quian
Director: Carlos José Elías Pérez

Facultad de Humanidades, Comunicación y Documentación
Departamento de Periodismo y Comunicación Audiovisual

Getafe, abril de 2016

Esta tesis doctoral se inscribe dentro del proyecto de investigación 'Big data, redes sociales y periodismo de datos: aplicación de las herramientas de monitorización al análisis de fuentes y contenidos periodísticos', financiado por el Ministerio de Economía y Competitividad dentro del Plan Nacional 'Proyectos de I+D+i, del Programa Estatal de Investigación, Desarrollo e Innovación orientada a los Retos de la Sociedad'. Referencia: CSO2013-47767-C2-1-R

Imagen de portada: composición creada con *Surveillance*, fotografía de Aubin Paul de la obra *Spy Booth* de Banksy, en una calle de Cheltenham (Inglaterra), y *Wikileaks _DDC1948*, de Thierry Ehrmann en el museo Demeure du Chaos, en Saint-Romain-au-Mont-d'Or (Francia). Ambas imágenes están bajo licencia Creative Commons Reconocimiento 4.0. Internacional (CC BY 4.0), disponibles en:
https://www.flickr.com/photos/aubinpaul/13851884344/
https://www.flickr.com/photos/home_of_chaos/5333126271/.

Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Impacto mediático y político del activismo hacker en la sociedad red. Estudio de caso: WikiLeaks

Autor: Luis Alberto Pampín Quian
Director: Carlos José Elías Pérez

FIRMA DEL TRIBUNAL CALIFICADOR

Firmas

PRESIDENTE:

VOCAL:

SECRETARIO:

CALIFICACIÓN:

Getafe, de de

A la memoria de mi madre y a Bárbara,
los dos faros que iluminan mi vida.

AGRADECIMIENTOS

Dar las gracias es para mí mucho más que una fórmula de cortesía o un simple protocolo, es un acto de aprecio profundo y de reconocimiento sincero a quienes me han prestado su sabiduría, su corazón y su compañía en el largo camino hasta aquí.

No hay palabras ni gestos de agradecimiento que puedan describir y expresar mi gratitud a mi director de tesis, Carlos Elías. Gracias por iluminarme, por despejar la niebla, por ampliar el horizonte, por el viento a favor. Gracias por al abastecimiento de ideas, por la transferencia de conocimiento, por el contagio de entusiasmo. Gracias por la confianza y por compartir la pasión. Gracias por ser mi maestro.

En la memoria de mi corazón están también todos los profesores que a lo largo de mi vida me han ilustrado y aconsejado sabiamente. Durante la escritura de esta tesis me han asaltado recuerdos que ahora me emocionan de los maestros del Colegio Público Doblada y de los profesores del IES Castelao de Vigo. Siento orgullo de haber estado en esas aulas y a todos ellos, a mis profesores, les quiero agradecer su encomiable labor. También vibrantes son los recuerdos que permanecen en mí de mi etapa en la Universidade de Vigo, donde hoy, junto con mis apreciados profesores, enseñan viejos compañeros de aventuras y desventuras universitarias. Mi infinito agradecimiento también a los profesores de la Universitat Oberta de Catalunya y de la Universidad Carlos III de Madrid por haber contribuido a reactivar mi pasión académica. A ellos, a todos, a los que ya no están y a los que siguen, gracias por haberme ayudado a llegar aquí.

Gracias a WikiLeaks por haberme invitado a participar en su red de investigadores.

Gracias a Richard Stallman por haber compartido conmigo su tiempo y su entusiasmo hacker.

Gracias a la ciudad de Manchester por darme la pausa, la inspiración y la perspectiva que necesitaba en un momento crítico. Y gracias a los emigrantes españoles que allí conocí, que escaparon de la desesperanza de un país deprimido, porque a ellos les debo haber recuperado la ilusión por reconquistar nuestro futuro.

Gracias a Concha por ser mi madre adoptiva, por espolearme, por apoyarme, por confiar en mí. Jamás podré agradecerle lo que ha hecho para que alcance mis sueños.

Gracias a mis ahijados y sobrinos Uxía, Lucas, Nico, Claudia, Noa y Carla, que me devolvieron el espíritu hacker que en todo niño subyace hasta que nos es arrebatado por la fuerza, y por los que siento un amor profundo. Y gracias a Adrián —mi hermano en el camino—, Susana, Ángel y Esther por compartir conmigo lo más importante de sus vidas.

Gracias a Miguel Núñez por no dejar que desfallezca, por estar siempre a mi lado y por su valerosa defensa de la dignidad como principio fundamental para la libertad del individuo.

Y a los tres seres que más quiero, por los que siento un amor eterno, a los pilares de mi universo, a mis fuentes de inspiración y de aliento, a los motorores de mi vida y de esta tesis, gracias por existir y por agitar mi espíritu inquieto: Bárbara, Ziggy y Lupita.

RESUMEN

Este trabajo de investigación traza la línea evolutiva de la cultura hacker que explica cómo y por qué surge el fenómeno WikiLeaks. Primero hacemos un análisis teórico, conceptual, histórico, interpretativo y crítico de la ética y la cultura hackers, y del hacktivismo como manifestación política del *hacking*. En esta aproximación identificamos las primeras fuentes documentales propias de la cultura hacker, las primeras referencias a hackers y hacktivistas en los medios de masas, y las primeras consecuencias sociopolíticas del desarrollo de una inteligencia colectiva hacker favorecida por el progreso de la computación, la aparición de Internet y la expansión de la sociedad red. A continuación describimos el ambiente informacional en el que se desarrolla la sociedad red y las condiciones que contribuyen a la aparición de WikiLeaks. En nuestro estudio de caso explicamos WikiLeaks como un nuevo modelo de organización-red transnacional y hacktivista, escarbamos en sus raíces políticas y detallamos su estrategia informativa y su relación con los medios de masas. También examinamos el *storytelling* aplicado en el debate público sobre WikiLeaks y Julian Assange, y revisamos experiencias transmediáticas que contribuyen a la propagación del universo WikiLeaks. Para explicar los procesos colaborativos de WikiLeaks utilizamos la metodología de observación participante, introduciéndonos en su red de colaboradores. Aportamos también datos de la actividad de WikiLeaks en Twitter y Facebook, de los registros de búsquedas sobre WikiLeaks en Google, de la evolución del tráfico estimado en su sitio web y de la actividad generada en su página de Wikipedia, así como de su impacto en las portadas de los cinco medios que colaboraron en el *Cablegate*. Además, sometemos al escrutinio de la lingüística computacional los discursos enfrentados de WikiLeaks y sus socios en las filtraciones de los cables diplomáticos de Estados Unidos. Pretendemos así dilucidar por qué surge WikiLeaks, cuál es su método y estrategia, cuándo y cómo alcanzó su máximo impacto mediático y político, cuáles son los retos que plantea este nuevo modelo de organización-red hacker en el campo de los medios de comunicación, en general, y del periodismo, en particular, y de qué manera contribuye a fortalecer el desafío que representa la ética hacker como espíritu alternativo para la sociedad red.

Palabras clave: ética hacker, hacktivismo, medios, periodismo, sociedad red, wikileaks.

ABSTRACT

This research tracks the evolution of hacker culture, which underlies how and why the WikiLeaks phenomenon came about. First, we perform a theoretical, conceptual, historical, interpretative and critical analysis of the hacker ethic and culture, and of hacktivism as politically-motivated hacking. Through this approach, we identify the first documentary sources pertaining to hacker culture, the first references to hackers and hacktivists in the mass media, and the first socio-political consequences of the development of collective intelligence among hackers. This collective intelligence has been underpinned by progress in computing, the emergence of the internet and the expansion of the network society. We go on to outline the informational environment that have given rise to the network society and the conditions that contributed to the emergence of WikiLeaks. In our case study, we describe WikiLeaks as a new transnational, hacktivist network organisation; we explore its political roots and highlight its information strategy and its relationship with the mass media. We also look at storytelling in the public debate around WikiLeaks and Julian Assange, and review the transmedia narratives that have contributed to the proliferation of the WikiLeaks universe. To explain WikiLeaks' collaboration processes, we used a methodology based on participant observation, joining its network of partners. We also provide information on WikiLeaks' activity on Twitter and Facebook, on Google search records about WikiLeaks, on the progression of the estimated traffic on its website and the activity generated through its Wikipedia page, as well as its impact on the front pages of the five media outlets that collaborated on Cablegate. We also use computational linguistics to scrutinise the competing discourses of WikiLeaks and its partners regarding the US diplomatic cable leaks. Our intention is to clarify why WikiLeaks emerged, what its method and strategy are, how and when it achieved its maximum media and political impact, what challenges stem from this new hacker network organisation in the media landscape in general and in journalism specifically, and how it contributes to intensifying the challenge represented by the hacker ethic as an alternative spirit for the network society.

Keywords: hacker ethic, hacktivism, journalism, media, network society, wikileaks.

ÍNDICE

> *Sí, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis.*
>
> —Loyd Blankenship 'The Mentor'.

INTRODUCCIÓN

1. OBJETO DE ESTUDIO Y MOTIVACIÓN

Los hackers han sido tradicionalmente estigmatizados como delincuentes informáticos. Los discursos de los tres poderes clásicos —ejecutivo, legislativo y judicial— y del cuarto poder —el periodismo— han impregnado el término *hacker* de un valor semántico negativo que lo coloca al margen de la ley, de las normas y convenciones sociales, y de cualquier código moral o ético. Sin embargo, contra esa visión distorsionada y reduccionista de los hackers, y del movimiento de hackers activistas (a partir de ahora, hacktivistas[1]) que ha surgido con la irrupción y popularización de Internet, de los llamados medios sociales en línea y del software libre, el estudio y análisis científico y riguroso del *hacking*, del hacktivismo y de los fenómenos, grupos, entidades o individuos hackers no sólo puede, sino que debe ser abordado, investigado y explicado desde distintos campos de estudio y conocimiento para, con las partes, llegar a una comprensión global del *hacking* y del hacktivismo sin prejuicios: desde el jurídico y legal hasta el político, filosófico, ético, mediológico, sociológico o informático.

Este trabajo propone liberarnos de prejuicios y del maniqueísmo característico del discurso dominante de los medios de comunicación de masas sobre los hackers para explicar, desde un enfoque teórico-crítico, la cultura y la ética hackers y su manifestación en los movimientos ciberactivistas, en el marco de la sociedad red, esto

[1] *Hacktivista* y *hacktivismo* son dos términos que se han popularizado y normalizado para referirse a aquellos hackers inmersos en el activismo político y social.

es, en la nueva "estructura social hecha de redes de información propulsadas por las tecnologías de la información características del paradigma informacionalista" (Castells, 2001b: 166). Con esta tesis pretendemos iluminar un fenómeno en efervescencia y connatural al desarrollo de las tecnologías digitales de la información y de la comunicación, de Internet y del ciberespacio, y que, pese a ello, ha subsistido en la opacidad impuesta por las estructuras de poder tradicionales.

En esta tesis intentamos describir uno de los componentes clave de la nueva geografía de poder, el hacktivismo, el cual sólo puede ser plenamente entendido en el contexto tanto de su patrimonio y herencia hackers como de las nuevas respuestas políticas innovadoras a las redes de comunicación de las sociedades virales. Nos introduciremos en sus métodos y en sus estrategias dirigidas a que la acción directa en línea se viralice hasta resultar en consecuencias políticas.

La idea de abordar un fenómeno tan complejo como el activismo hacker en la sociedad red se presumía una tarea ardua por cuanto aún hoy es difícil encontrar un acuerdo social sobre qué es ser hacker, qué función social cumplen los hackers y qué papel juega la nueva generación de hackers —los hacktivistas— en los procesos de cambio social, económico, político y mediático en un nueva realidad que se configura por la interacción entre la realidad física y la virtual, y que fluye por las redes de comunicación. También delicada, ya que el valor semántico delictivo que se ha impuesto al hacker —y, por ende, al hacktivista— parece condicionar y predisponer cualquier enjuiciamiento sobre este asunto, hasta el punto de obligar al investigador a realizar un esfuerzo adicional en la justificación del objeto de estudio para que no intercedan ni intoxiquen en la valoración e interpretación tabús, convencionalismos y prejuicios asentados por los medios de masas y los poderes tradicionales que confunden a la opinión pública.

No es objeto de este trabajo ser defensa ni acusación, ni siquiera juzgar al hacker y, en concreto, al hacker como activista sociopolítico. Tampoco lo es cuestionar ni defender la jurisprudencia existente ni intentar articular un discurso jurídico. Simplemente partimos de la premisa de que ser hacker no conlleva una mancha delictiva por definición. Ahora bien, sí es cierto que ciertas actividades de los hackers suponen transgresiones legales, aunque entendemos que se producen no sólo en pro de un bien común —como defiende la comunidad hacktivista—, sino además por la

mutabilidad de una nueva realidad, la hiperrealidad que se está conformando con el uso de las tecnologías digitales, de los nuevos espacios de interacción y de la fricción entre el espacio físico y el ciberespacio (o espacio virtual), que está transfigurando nuestras vidas, nuestras identidades, nuestras relaciones sociales, nuestros trabajos y el funcionamiento de la economía, de la política, del Estado-nación y de las democracias. Entendemos que esa mutabilidad debe ser correspondida con nuevos ordenamientos jurídicos adaptables a la nueva realidad cambiante a la que nos enfrentamos y, por ello, son vastos los retos que tienen por delante legisladores y juristas para dar orden a una realidad líquida, global y transnacional, difícil de encajar y acoplar en la idea tradicional del Estado-nación roGrademocrático, en su ordenamiento jurídico y en la vieja geografía política, que se ven ahora desbordados por la sociedad red y la nueva conceptualización del mundo.

Arrojar luz sobre el *hacking* y el hacktivismo es una de las obsesiones no sólo de la comunidad hacker, sino también de muchos estudiosos que se han afanado en repasar su verdadera historia, relatar sus hitos y fracasos, y describir sus pasiones y valores para clarificar su verdadero estatus y función social. Pero los "héroes de la revolución computacional" —como los definió el periodista Steven Levy en 1984— han tenido muy mala prensa y su nefasta reputación ha sido heredada por las nuevas generaciones de hackers que se han pasado al activismo ciberespacial. "La prensa ha dramatizado la vulnerabilidad de la sociedad a las debilidades en seguridad informática agrupando vagamente fenómenos tan dispares como hacktivistas, terroristas y virus informáticos y biológicos" (Jordan y Taylor, 2004: 21).

Para acercarnos al hacktivismo y a sus intricadas y complejas relaciones con el poder, estudiamos el fenómeno WikiLeaks como paradigma hacktivista informacional. Los orígenes de esta organización transnacional, sus raíces filosóficas y éticas, sus relaciones con los medios de comunicación convencionales y los periodistas, sus filtraciones masivas de documentos secretos, sus estrategias de impacto mediático y político, y sus efectos vertebran nuestro caso de estudio, con el que pretendemos dilucidar cómo los nuevos hackers contribuyen a una nueva transformación radical de nuestra sociedad desde la acción política, al igual que hicieron sus predecesores desde la transformación tecnológica. En definitiva, intentaremos profundizar en el valor transformativo del hacktivismo mediante el estudio del fenómeno WikiLeaks.

En los últimos años, la organización WikiLeaks ha ocupado portadas de periódicos y revistas de todo el mundo, ha abierto informativos de las principales cadenas de televisión, ha sido objeto de numerosos reportajes y documentales, y se ha virazilizado en Internet, además de generar una extensa colección de libros y guiones cinematográficos centrados en la figura de su fundador —el hacker australiano Julian Assange— y en el fenómeno de las filtraciones masivas de documentos secretos de gobiernos y corporaciones transnacionales.

Después de tres años de actividades, WikiLeaks y su fundador alcanzaron notoriedad mundial en el año 2010 con una serie de filtraciones masivas de documentos secretos relacionados con las guerras en Irak y en Afganistán, pero sobre todo, con las revelaciones del famoso caso *Cablegate* sobre los entresijos de la política exterior de Estados Unidos, que se hicieron públicos con la filtración de miles de cables diplomáticos entre el Pentágono y las embajadas estadounidenses repartidas por todo el mundo. WikiLeaks decidió entonces aliarse con cinco grandes medios de comunicación escritos de Occidente, globales y tradicionales, para publicar los contenidos de aquellos cables. *The New York Times* (Estados Unidos), *The Guardian* (Reino Unido), *Der Spiegel* (Alemania), *Le Monde* (Francia) y *El País* (España) trabajaron conjuntamente para sacar a la luz la mayor filtración de documentos secretos jamás revelados sobre la diplomacia de Estados Unidos. Aquella fue también la mayor y más importante colaboración entre medios de información en la historia del periodismo.

Las filtraciones de WikiLeaks han causado una convulsión política y mediática mundial, y han generado apasionados debates todavía vigentes sobre las bondades o perversidades de Julian Assange y de su organización, sobre la legitimidad de revelar secretos de Estado y corporativos, sobre la transparencia política y el derecho a la libre información y a la libertad de expresión, sobre las estrategias para ahogar económicamente a WikiLeaks y a cualquier organización informativa que pretenda subvertir las estructuras y sistemas de poder tradicionales de los Estados-nación y sus mecanismos de información, y sobre los desafíos que plantea WikiLeaks a los medios de comunicación tradicionales y a los periodistas como vigilantes del poder (*watchdog*), en un contexto, el actual, en el que la crisis de identidad, de credibilidad y de negocio del periodismo genera enormes incertidumbres sobre este sector, inmerso en un proceso de reconversión.

Este trabajo debe ayudar, por lo tanto, no sólo a clarificar qué es, cómo se configura y qué causas defiende el hacktivismo; también debe contribuir a conocer y comprender el fenómeno WikiLeaks, la intrincada personalidad y pensamiento político de su fundador, Julian Assange, y, sobre todo, debe contribuir a dilucidar sus estrategias y tácticas para lograr sus objetivos de máximo impacto mediático y político, para lo cual, "el análisis de las lógicas narrativas puede arrojar luz sobre la formación pública de fenómenos como WikiLeaks, incluyendo las técnicas utilizadas tanto para su represión como para su transmisión con éxito" (Uricchio, 2014: 2571)[2].

Esta investigación busca también motivar nuevas líneas de investigación sobre un nuevo paradigma cultural que trasciende a WikiLeaks y a Julian Assange y que, en definitiva, supone un replanteamiento de la democracia y de los derechos de los individuos a comunicarse, informar y conocer libremente.

[2] Todas las citas tomadas de Uricchio (2014) en esta tesis son traducciones propias del texto original, en inglés.

2. OBJETIVOS E HIPÓTESIS

2.1. Objetivos de la investigación

El objetivo general de esta tesis es describir la lógica evolutiva de la cultura hacker, explicar sus dimensiones ética y política, y analizar su impacto con un enfoque mediológico, para intentar dilucidar *cómo* y comprender *por qué* surge un fenómeno como WikiLeaks en la era de la sociedad red.

Para aproximarnos al universo WikiLeaks era fundamental primero explorar los fundamentos éticos, culturales y políticos que subyacen a su aparición. Entendimos que era necesario primero revisar la historia hacker y aportar una mirada nueva y profunda —desde la investigación académica en español en medios de comunicación— a la ética y cultura hackers, a su lógica evolutiva —determinada por el desarrollo de las tecnologías digitales de la información y de la comunicación, y por las emergencias sociopolíticas de nuestro tiempo—, y al enfoque mediático y a la lectura política que se ha hecho del *hacking*.

Este trabajo parte de la premisa de que no se puede explicar nuestro caso de estudio, WikiLeaks, sin explorar primero los fundamentos éticos, culturales y políticos que subyacen a su aparición, y su exposición en los medios de comunicación, es decir, sin abordar en profundidad la historia y el impacto social de la cultura hacker y de los movimientos ciberactivistas surgidos en su seno o inspirados por ésta.

Este recorrido necesita, además, ser enmarcado en el paradigma tecnológico dominante de nuestra sociedad actual, el informacionalismo, que está sustituyendo al industrialismo, y del cual brota la sociedad red, siendo uno de sus componentes fundamentales la "fuente cultural de innovación tecnológica representada por la cultura hacker" (Castells, 2001b: 177).

Una vez trazadas las conexiones de WikiLeaks con la cultura y el activismo hackers, en el marco de la sociedad red, podemos intentar resolver algunas de las muchas interrogantes que plantea como organización apátrida y en red, adscrita a la ética hacker y a la defensa de los derechos humanos.

El objetivo principal de nuestro estudio de caso es elucidar la estrategia de WikiLeaks para lograr el máximo impacto mediático que facilite el máximo impacto político de su mensaje. Para ello, pretendemos:

- Averiguar cuándo y cómo alcanza WikiLeaks su máximo impacto mediático.
- Analizar cómo funciona una organización en red y desterritorializada como WikiLeaks en los procesos de producción, publicación y difusión de la noticia, y observar cómo se relacionan en estos procesos la ética hacker y la ética periodística.
- Ahondar en la relación de un nuevo tipo de organización en red, transnacional y desterritorializada como WikiLeaks con los medios de comunicación de masas tradicionales, y dilucidar qué les une y qué les separa.
- Contribuir a responder quién es Julian Assange y qué es WikiLeaks, qué dicen y hacen, a quién van dirigidos sus mensajes, con qué objetivos y con qué consecuencias.
- Desentrañar las estrategias de WikiLeaks y las respuestas de sus partidarios y detractores.
- Explicar las filtraciones de WikiLeaks como fenómenos transnacionales y transmediáticos, con efectos también locales o regionales.

2.2. Hipótesis

- H1: El desarrollo y democratización de la Red y de tecnologías digitales de la información y la comunicación son decisivos en el progreso de la ética y la cultura hackers como espíritu alternativo para la sociedad red, y en la manifestación de la dimensión política del *hacking*. En este proceso, WikiLeaks marca un nuevo estadio evolutivo hacker.
- H2: WikiLeaks propone un nuevo modelo de organización red, líquida y transnacional para un nuevo periodismo colaborativo, descentralizado, apasionado, activista y comprometido con la ética hacker, la transparencia y la defensa de los derechos humanos, frente al modelo de periodismo competitivo, industrializado, mercantilizado, rutinario, jerarquizado y comprometido por las cuentas de resultados.

- H3: El medio —WikiLeaks— es el mensaje, y el mensaje es subvertir la estructura tradicional de los poderes político y mediático, y desmantelar el secreto como mecanismo de poder de los Estados-nación y de las corporaciones empresariales.
- H4: La simple liberación masiva de información y de datos en bruto no es eficaz para impactar en la opinión pública. Las labores clásicas del periodismo siguen siendo necesarias para asistir informativamente a las masas no ilustradas en el acceso, verificación, tratamiento, análisis e interpretación de la información y de los datos en bruto.
- H5: En la era de la sociedad red, los medios tradicionales de masas siguen siendo dominantes y claves para lograr el máximo impacto político de un mensaje. La colaboración sin precedentes de cinco medios generalistas globales y tradicionales es decisiva en la legitimación, popularización e impacto en la esfera pública de WikiLeaks y de Julian Assange.
- H6: El objetivo principal de Julian Assange es conseguir el máximo impacto político en Occidente, donde se juega su crédito y autoridad, y esto sólo es posible a través de la prensa generalista más influyente en los cuatro idiomas más poderosos en la cultura occidental: inglés, francés, español y alemán.
- H7: Los medios de comunicación han contribuido a desviar la atención del mensaje —WikiLeaks— y a focalizar el interés en el mensajero —Julian Assange— para rentabilizar el fenómeno WikiLeaks.
- H8: La historia de Julian Assange es el resultado de la aplicación de estrategias narrativas transmediáticas destinadas a convertir al líder de WikiLeaks en héroe o villano, según el tradicional sistema de antinomias u oposiciones binarias que han contrbuido a organizar una comprensión y evaluación social del *hacking* y del hacktivismo.

3. ANTECEDENTES Y ESTADO ACTUAL DEL TEMA

Cuando nos enfrentamos a este caso de estudio ya éramos consicientes de que sobre WikiLeaks y Julian Assange existía una extensa literatura ensayística, periodística y biográfica que iría *in crescendo* exponencialmente a la par que los acontecimientos alrededor de WikiLeaks se iban sucediendo en avalanchas de información periodística que darían lugar más tarde a más literatura comercial, a una cada vez mayor producción científica, a una variada filmografía, etc. Toda una variedad de aproximaciones y enfoques, con puntos de vista divergentes, que han contribuido, con distintos relatos sobre los hechos, pero también con manifiestas opiniones y especulaciones, a situar el fenómeno WikiLeaks como uno de los de mayor impacto mundial de este siglo y uno de los acontecimientos más destacados de la historia del periodismo moderno.

Entre la vasta producción literaria encontramos numerosos libros que han ido apareciendo en el mercado literario desde principios de 2011, entre otros, los primeros y más destacados: *Inside Julian Assange's War on Secrecy* (2011), escrito por los periodistas de *The Guardian* David Leigh y Luke Harding; *Open Secrets. WikiLeaks, War and American Diplomacy* (2011), libro coral de *The New York Times* con aportaciones de reporteros, de analistas y del exeditor Bill Keller; *Julian Assange: The Unauthorised Autobiography* (2011), una polémica autobiografía editada por Canongate Books y escrita, tras horas de entrevistas con Assange, por Andrew O'Hagan, quien decidió no firmar la obra tras romperse el acuerdo al que se había llegado con el fundador de WikiLeaks por el que éste revisaría el contenido antes de su publicación; *Desmontando WikiLeaks*, una controvertida mirada del escritor superventas Daniel Estulin, exagente de contraespionaje del KGB; *The Most Dangerous Man in the World*, biografía sobre Assange del periodista australiano Andrew Fowler; *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website* (2011), de Daniel Domscheit-Berg, excolaborador de Assange y fundador de OpenLeaks (clon de WikiLeaks), considerado por Assange y sus seguidores un traidor resentido; o *W de WikiLeaks. La venganza contra las mentiras del poder* (2011), de Bruno Cardeñosa, director de la revista española *Historia de Iberia Vieja* y presentador del programa radiofónico *La Rosa de los Vientos*, que se emite en Onda Cero.

Lo cierto es que cuando abordamos esta investigación, la producción literaria comercial sobre el fenómeno WikiLeaks empezaba a ser amplia, pero no era tan

abundante la producción científica. La aplicación de métodos y técnicas de investigación científica sobre este tema no abundaba y en algunos casos WikiLeaks y Assange aparecían de forma tangencial. En la primera literatura científica encontrada, cuando pusimos en marcha este proyecto de investigación, observamos que había una escasez de estudios en los que se aplican técnicas cuantitativas e intuimos un escaso afán por el análisis estadístico y la recolección e interpretación de datos sistemática. Por el contrario, vimos que había un predominio de análisis conceptuales, históricos, documentales y de contenido con enfoques mayoritariamente cualitativos.

A continuación recogemos una muestra de los primeros textos sobre WikiLeaks que hallamos en el ámbito científico-académico, en nuestra primera exploración en los orígenes de esta investigación.

Cuadro 1: Muestra de la primera literatura científica encontrada sobre el fenómeno WikiLeaks.

	Título	Autor	Publicación	Resumen	Metodología
1	The Battle of WikiLeaks: Mass Self-Communication, Hacker Culture, and Financial Institutions.	Nur Uysal, University of Oklahoma.	24rd Annual International Association of Conflict Management Conference. Istanbul, Turkey. July, 3 – 6, 2011.	In 2010, WikiLeaks raised considerable discussion over the disclosure of sensitive documents to the public domain (Gellman & Harrell, 2010; Ludlow, 2010). Whether WikiLeaks is a media organization dedicated to bring important news and information to the public as WikiLeaks members claimed is questionable. Yet, it is a reality that Wikileaks is a network society emerged around a global web of horizontal communication networks that exchange information. It acts as an alternative media as well as a form of social movement that aims to change power relations in the society. This paper examines Castells's mass self-communication thesis (2007, 2009) which argues that in the age of network society although the media do not hold power per se, they have become the social space where power is decided. Though the importance of mainstream media coverage for firm valuation has been well-documented, relatively little is known about the impact of as mass self communication - new horizontal and digital communication network - on stock values. As an attempt to fill this gap, this study investigates the influence of recent WikiLeaks disclosure on the stock market values of banking industry, in particular on Bank of America. The results of an event study analysis showed that Wikileaks indeed had an impact on Bank of America's abnormal return. Specifically, Bank of America hit the lowest value (under $11) since 2009 following the interview on November 30, 2010.	Estudio de caso: evaluar matemáticamente, a través de ecuaciones, las reacciones anormales del mercado y el comportamiento de los precios de las acciones del Bank of America tras el anuncio de WikiLeaks de la fecha de publicación de una filtración sobre el comportamiento inmoral de un gran banco de EE.UU., y el posterior anuncio de que esa filtración se vinculaba al Bank of America.
2	Online Storytelling: Studying Homo narrans in several online habitats by analyzing the framing of the Wikileaks Iraq video in newspapers, blogs and tweets.	Jelmer Mommers, University of Groningen.	Research seminar: Citizen/Journalism: User Generated Content and the Consequences for Journalism. Module: LJX031M10. June 6, 2010. Master of Journalism, University of Groningen.	Working within the narrative paradigm as posited by Walter Fisher in 1985, a framing analysis was conducted to map the reception of the Wikileaks Iraq video by American newspapers, professional news blogs and by people on Twitter. The idea is that not only journalists, but all people are storytellers. Studying their storytelling on different online platforms, we can learn about the politics of form of these media, about their functions, and about the storytelling behaviour of different online users, who function within different institutional contexts. The analysis showed that several different versions of the Wikileaks Iraq video story existed online. It showed that people will tell one story or the other dependent on the context of their production, and dependent on the medium they use. People on different platforms were shown to make meaning differently. This tells us yet again that homo narrans, man the storyteller, is flexible.	Estudio de caso: análisis del vídeo de la guerra de Irak publicado por WikiLeaks en el que soldados de EE.UU. asesinaron a doce personas desde un helicóptero Apache, y examen de su recepción y narración en medios tradicionales y plataformas *online* (teoría del *framing*): los 10 periódicos en papel y online y los blogs políticos más populares en EE.UU., y 200 actualizaciones en Twitter.

3	WikiLeaks 2010: A Glimpse of the Future?	Tim Maurer, Harvard Kennedy School.	Harvard's Belfer Center for Science and International Affairs, August 2010.	The recent publications on WikiLeaks reveal a story about money, fame, sex, underground hackers, and betrayal. But it also involves fundamental questions regarding cyber-security and foreign policy. This paper argues WikiLeaks is only the symptom of a new, larger problem which is the result of technological advances that allow a large quantity of data to be 'stolen' at low or no cost by one or more individuals and to be potentially made public and to go 'viral', spreading exponentially online. From this flows my assessment that the unprecedented quantity constitutes a new quality, "a difference in quantity is a difference in kind." Therefore, we need to delink WikiLeaks from Julian Assange for a serious discussion of the policy implications. Assange, himself, could represent the revival of a modern version of anarchism challenging governmental authority. First, I outline a conceptualization of the process of leaking. This part weaves the chronology of WikiLeaks into the discussion of the source, publisher, and an examination of the role of mainstream media, including references to Daniel Ellsberg and the Pentagon Papers. In the second part I enlarge the frame to look at the issues that emerge once a leak has occurred and the government's response. Third, I examine the cyber-security implications since WikiLeaks' early releases only brought to public light what seems to already be known in the shadow world of government espionage, raising larger questions about cyber-security and foreign threats.	Análisis conceptual del proceso de filtración, análisis historiográfico y cronológico del fenómeno WikiLeaks.
4	On Wires and Cables: Content Analysis of WikiLeaks Using Self-Organising Maps.	Rudolf Mayer and Andreas Rauber, Institute of Software Technology and Interactive Systems, Vienna. University of Technology, Austria.	Jorma Laaksonen and Timo Honkela, editors. Proceedings of the 8th Workshop on Self-Organizing Maps (WSOM'11), volume 6731 of Lecture Notes in Computer Science, pages 238-246. Springer Berlin / Heidelberg, June 13-15 2011.	The Self-Organising Map has been frequently employed to organise collections of digital documents, especially textual documents. SOMs can be employed to analyse the content and relations between the documents in a collection, providing an intuitive access to large collections. In this paper, we apply this approach to analysing documents from the Internet platform WikiLeaks. This document collection is interesting for such an analysis for several aspects. For one, the documents contained cover a rather large time-span, thus there should also be an quite divergence in the topics discussed. Further, the documents stem from a magnitude of different sources, thus different styles should be expected. Moreover, the documents have very interesting, previously unpublished content. Finally, while the WikiLeaks website provides a way to browse all documents published by certain meta-data categories such as creation year and origin of the cable, there is no way to access the documents by their content. Thus, the SOM offers a valuable alternative mean to provide access to the content of the collection by their content. For analysing the document collection, we employ the Java SOMToolbox framework, which provides the user with a wealth of analysis and interaction methods, such as different visualisations, zooming and panning, and automatic labelling on different levels of granularity, to help the user in quickly getting an overview of and navigating in the collection.	Análisis de contenido de la página web de WikiLeaks a través de mapas autoorganizados o SOM (Self-Organizing Map).

5	Case study of the Wikileaks Whistleblower.	R. Lennon.	Dublin City University, December 10, 2010	The ethical debate for the whistleblowing of the US-Embassy cables has shown two very strong sides, and from the questions raised in this paper it can be seen that there is issues with both the US military and diplomatic actions, the handling of the case by the State Department, the way the cables were leaked, and the way the cables were handled/published. A method is applied to clear the debate from an ethical point of view, and includes some of the latest news reports as the new batch of cables announced at the end of November continues to be released.	Estudio de caso: aplicación de la metodología *top-down* o de etapas de refinamiento de Blaise W. Liffick para un análisis del escenario ético.
6	Analogías de la Historia I: Julian Assange y Wikileaks *vs* Daniel Ellsberg y los Pentagon Papers.	Carlos Sánchez Hernández.	Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas. Universidad Complutense de Madrid, 31 de marzo de 2011.	En noviembre de 2010 el mundo entero contempló estupefacto el espectáculo de 250.000 documentos clasificados como "alto secreto", la mayoría pertenecientes al gobierno de Estados Unidos, que mostraban al mundo y de forma desnuda los entresijos de los últimos años de la diplomacia mundial, y en su vertiente más oscura. El responsable de la mayor filtración de documentos oficiales de la historia era Julian Assange, un "hacker" informático experto en indagar en material secreto e inaccesible, que creó en diciembre de 2006 "Wikileaks" (aunque inició sus actividades en Julio de 2007), una red de información a nivel mundial y a modo de foro que cuenta con hasta tres millones de colaboradores y potencialmente cientos e incluso miles de millones de lectores. En este trabajo se analizan las enormes similitudes entre esta enorme filtración de secretos oficiales llevada a cabo por Wikileaks a lo largo de 2010, y la sorprendente filtración que hizo Daniel Ellsberg en 1971, ambos hechos enclavados en sendas guerras que a su vez tienen también grandes similitudes: la guerra de Vietnam y la actual Guerra Contra el Terrorismo escenificada en Irak y Afganistán.	Análisis histórico comparativo.

7	"The Assange Effect": WikiLeaks, The Espionage Act and the Fourth Estate.	Shaina Jones and Jay Ward Brown.	Media Law Resource Center Bulletin, August 2, 2011.	This paper examines what might be required to sustain a prosecution of Assange under the Espionage Act and the possible legal impact of such a prosecution on traditional news organizations. In Part I, we briefly trace Assange's biography and provide an overview of WikiLeaks. In Part II, we discuss the history of and public policy behind the Espionage Act, and examine what the government would be required to prove in order successfully to prosecute Assange, including whether the First Amendment might provide a defense to such a prosecution. In Part III, we briefly consider how prosecution of Assange might differ under the Official Secrets Act in Great Britain (on which the American Espionage Act is in part based) if the leaked materials had belonged to the British government. Finally, in Part IV, we consider how the WikiLeaks affair has affected newsgathering more generally, including the adoption by some mainstream media organizations of information-gathering apparatus similar to that employed by WikiLeaks	Análsis narrativo-biográfico e histórico.
8	Los tres derrumbes y la nueva configuración geopolítica de la seguridad en internet. La caída del muro de Berlín, el 11/9 y Wikileaks.	Juan Manuel Fernández Chico.	Razón y palabra, Nº 75, 2011.	Este artículo intenta hilas tres momentos claves en la historia de la geopolítica de la seguridad: la caída del muro de Berlín, el ataque del once de septiembre de 2001 al World Trade Center y las recientes filtraciones del Departamento de Estado por parte de la organización Wikileaks, para trazar cómo el proyecto de protección global a través del miedo, encabezado por Estados Unidos, legitima sus acciones geopolíticas, ahora impactando también en la Internet, justificándolo por medio de la amenaza a su seguridad nacional.	Análisis histórico comparativo.

9	Digital Whistleblowing in Restricted Environments.	Graeme B. Bell.	JoDI: Journal of Digital Information. Vol. 12, Nº. 3, 2011.	The exposure of an organisation's illegal or unethical practices is often known as whistleblowing. It is currently a high- profile activity as a consequence of whistleblowing websites such as Wikileaks. However, modern digital fingerprinting technologies allow the identification of the human users associated with a particular copy of a leaked digital file. Fear of such discovery may discourage the public from exposing illegal or unethical practices. This paper therefore introduces the novel whistleblower-defending problem, a unique variant of the existing document- marking and traitor-tracing problems. It is addressed here by outlining practical steps that real-world whistleblowers can take to improve their safety, using only standard desktop OS features. ZIP compression is found to be useful for indirect file comparison, in cases where direct file comparison or use of checksums is impossible, inconvenient or easily traceable. The methods of this paper are experimentally evaluated and found to be effective.	Análisis experimental y comparativo de métodos y técnicas para realizar filtraciones de documentos digitales comprimidos de forma segura.
10	The News Production Process about the U.S. Embassy Cables: How 'The Guardian', 'The New York Times' and 'El País' Covered and Released the Documents Provided by WikiLeaks.	Miguel Carvajal, José Alberto García Avilés, José Luis González Esteban.	Diversity of Journalisms. Proceedings of the ECREA Journalism Studies Section and 26th International Conference of Communication (CICOM) at University of Navarra, Pamplona, 4-5 July 2011.	In November 2010, WikiLeaks provided 250,000 diplomatic documents to five news organisations throughout the world. The United States diplomatic cables leak (also known as "Cablegate") has sparked the debate about the journalistic nature of WikiLeaks and about transparency and free speech. However, it is a great opportunity to see how the press covered and reported the documents by analysing the strategies and practices of three newspapers. It also provides comparative material to establish differences not only between newspapers, but also countries, media cultures and journalists. The methodology uses comparative data gathered from each newspaper through questions that address the main aspects of the news production process: the agenda of negotiations with Julian Assange (founder of WikiLeaks); the publication schedule; decision making and the ethics about the publication of compromising cables; how the staff was managed and coordinated, and what types of guidelines were given; the ombudsman policy regarding the publication of the cables; etc. This paper describes how three major news media organise their news production in a situation that is different from the regular daily basis. This case gives us an excellent opportunity to analyse how different editors drew up a plan for the publication of one of the most important leaks in the recent history of public opinion.	Análisis de contenido comparativo de las publicaciones en los tres principales periódicos colaboradores de WikiLeaks durante el *Cablegate*: *The Guardian*, *The New York Times* y *El País*.

11	Getting Personal: Personification vs. Data-Journalism as an International Trend in Reporting about Wikileaks.	Andrea Czepek.	Diversity of Journalisms. Proceedings of the ECREA Journalism Studies Section and 26th International Conference of Communication (CICOM) at University of Navarra, Pamplona, 4-5 July 2011.	Data-journalism has been hailed as a new trend in reporting, but the case of WikiLeaks shows that due to economic, political and media-related conditions, personification and scandalization prevail in journalism. Instead of investigating into the large amount of information WikiLeaks has made available, most mainstream-media soon focused on the hunt for WikiLeaks' representative Julian Assange, while they largely ignored the content of the published material itself. Based on a comparative content analysis of several European news media in December 2010, this presentation will show that the emphasis on prominent individuals and personified, un-political aspects of a story rather than in-depth analysis of complicated contexts is an international trend. Despite different journalism cultures, media systems, political and economic conditions, and despite the possibilities the internet provides (publication of masses of data, crowd-sourcing its evaluation), there is an internationally homogeneous trend towards superficial, sensational, human-interest oriented and personified news, rather than a diversity of approaches. The Internet provides new possibilities for investigative journalism: Masses of data can be made public anonymously on platforms like WikiLeaks; crowds of people can analyze masses of data which a few individuals alone could not handle. There are obvious chances for the democratic role of news media: Grievances can be disclosed that would otherwise remain obscure, and it becomes harder to hide irregularities. Aside from political concerns such as disclosure of security-relevant secrets, there are also difficulties: Data-journalism is resource-intensive. Many skilled investigators are needed to evaluate and double-check data. Data-evaluation is time-consuming and defies short-term deadlines. The processes revealed may be considered less "newsworthy" and more complicated to explain to readers than spectacular crime news. Complicated data are more difficult to understand and less sensational than personalized human-interest oriented news. Thus, readers' immediate attention is drawn more to the spectacular, conflictual, personified news. Economic aspects are twofold: Personified news is easier and cheaper to produce (less effort, time and personnel needed for research; less complicated matter to understand and analyze). And personified news is more popular, draws more immediate attention and thus readers and potential advertising revenue.	Análisis de contenido comparativo de medios de comunicación de Francia, Alemania, España, Suecia y el Reino Unido, seleccionados sobre criterios de calidad, relevancia y vínculos con WikiLeaks. Se analizaron 1.125 noticias (artículos en periódicos y noticias de televisión), en las se que mencionó a Wikileaks, publicadas entre el 1 y 31 de diciembre 2010.

12	The Hybrid Media System.	Andrew Chadwick.	European Consortium for Political Research General Conference, Reykjavik, Iceland, August 25, 2011.	This paper combines theory and empirical analysis to explore recent systemic change in the nature of political communication. Drawing on evidence from Britain and the United States on the changing relationships among politicians, media, and publics, I argue for the concept of the hybrid media system. This system is built upon interactions among old and new media and their associated technologies, genres, norms, behaviors, and organizations. Actors in the hybrid media system are articulated by complex and evolving power relations based upon adaptation and interdependence. We now require a holistic approach to the role of information and communication in politics –one that does not exclusively focus on new or old media, but instead empirically maps where the distinctions between new and old matter, and where they do not. The focus of my attention in this article is news. First, I outline an ontology of hybridity. Next, I discuss assemblages of hybridized news making. Then I examine the phenomenon of WikiLeaks as an example of power and interdependence in the construction of news	Enfoque teórico y empírico. Análisis conceptual de la hibridación aplicado a los medios y estudio de caso: WikiLeaks.
13	Pirate culture and hacktivist mobilization: The cultural and social protocols of #WikiLeaks on Twitter.	Simon Lindgren, Ragnar Lundström.	New Media and Society, vol 13, no. 6, September 2011.	This article uses the case of Twitter activity under the #WikiLeaks hashtag to address issues of social movements online. The aim is to analyze the potential of elusive web spaces as sites of mobilization. Looking at linguistic and social aspects, our main questions were: What are the characteristics of the communication in terms of common discursive codes versus fragmentation? In what respects can social order be distinguished, and to what extent are connections between users simply random? Are there any prominent patterns as regards the commitment of participators over time? With the help of tools from semantic, social network and discourse analysis, we were able to show that common codes, networks of connections and mobilization do exist in this context. These patterns can be seen as part of the elaboration of a 'cognitive praxis'. In order to organize and mobilize, any movement needs to speak a common language, agree on the definition of the situation and formulate a shared vision. Even though it is global and loosely-knit, Twitter discourse is a space where such processes of meaning-production take place.	Estudio de caso: análisis de contenido semántico en Twitter a través de herramientas de monitorización.

14	WikiLeaks CableGate and the Multi-Stakeholder Model of Internet Governance.	Julia Velkova.	Communication for Development (ComDev 09), Malmö University.	Internet is recognised as an alternative media tool that has the potential to stimulate civic cultures, mobilize and sustain civil society networks. It is also perceived as an important tool for social change that offers a powerful communication platform for different social groups to advance their views and ideology online in a significantly less controlled way than it is done through traditional media. In the end of 2010, the release of U.S. secret diplomatic on the Internet by the non-profit organisation WikiLeaks got an instant global outreach through the Internet and primarily, through the Wikileaks website – www.wikileaks.org. The immediate reaction to this resulted in governmental pressure on global providers of Internet services to stop servicing the website, thus preventing the global public from accessing the materials. The project studies the discussion that has arisen in the context of these actions and examines the communication tactics used by civil society and governmental actors in this discussion in order to advance an ideology of the right to communicate, and civil society participation in forming and safeguarding Internet principles. The project looks deeper at ideological, participatory, and developmental issues brought up in the discussion around the restriction of access to the main Wikileaks website, and how do they relate to eventual processes of social change. The study is based on Fairclough's framework on critical discourse analysis, and is grounded in the theoretical framework of participation, discourse and ideology. The main conclusion of the study is that the discussion around the Wikileaks CableGate case has clearly articulated the necessity of common Internet principles and democratic framework built in an inclusive and participatory manner through the active involvement of civil society actors in order to preserve the core values and enabling potential of Internet as media, and that an effective model for this is the multi-stakeholder model of Internet governance.	Estudio de caso: análisis de contenido, entrevistas estructuradas a representantes de ONG que reivindican gobiernos abiertos y flujo libre de la información, y grupos de hacktivistas; análisis crítico del discurso en el debate sobre el acceso a WikiLeaks.
15	La denuncia social en Internet: Wikileaks y la filtración de documentos secretos.	Javier Vidal Vega, José Romero Portillo.	Actas – II Congreso Internacional Latina de Comunicación Social – Universidad La Laguna, diciembre de 2010.	Desde la creación de Wikileaks en diciembre de 2006, este portal de Internet se ha convertido en un espacio de denuncia social empleado por ciudadanos de todo el mundo. A través de la web, los usuarios difunden documentos que desvelan comportamientos censurables de gobiernos, poderes públicos y empresas multinacionales. Al modo de la enciclopedia participativa Wikipedia, permite a los internautas alojar anónimamente, mediante conexión cifrada, textos, audios o vídeos confidenciales. El presente trabajo pone de manifiesto la capacidad de Wikileaks para propagar casos comprometidos, así como su valor de fuente para periodistas.	Estudio de caso: revisión bibliográfica, aproximación teórica, análisis de contenido de algunas filtraciones en el portal de WikiLeaks.

16	Wikis: Las comunidades del conocimiento.	Ana Lilia Careaga Mercadillo.	Instituto Tecnológico de Teléfonos de México S.C., diciembre 2010.	The term "wiki" comes from the Hawaiian word for "fast." Wiki technology creates a webpage that anyone with access to it can modify –quickly and easily. A wiki is essentially a webpage with an edit button. So, a wiki is just a website that allows the easy creation and editing of any number of interlinked web pages via a web browser using a simplified markup language. Community-based organizations, governments, schools/universities, and businesses are using wikis. The most famous wiki is Wikipedia, a free, multilingual, open content encyclopedia project. In this article you will find a full description of the concept of wiki, its applications and some of the tools that are available in the Net.	Análisis conceptual de WikiLeaks y del fenómeno *wiki*.

Fuente: elaboración propia.

Pese al gran impacto mediático de WikiLeaks desde el año 2010, observamos que había un déficit científico sobre este fenómeno en España, pero también en el resto del mundo, siendo particularmente interesante en el ámbito académico estadounidense, condicionado por las enormes tensiones políticas y jurídicas que han suscitado las filtraciones de WikiLeaks en este país. Así, por ejemplo, en la base de datos de la International Studies Association no se encontró ninguna publicación sobre WikiLeaks o derivada de los materiales filtrados por esta organización.

La International Studies Association es una reputada organización que fue fundada en el año 1959 para promover la investigación y la educación en los asuntos internacionales y que fomenta vínculos entre académicos y profesionales alrededor de los grandes fenómenos, conflictos y procesos mundiales de transformación de la humanidad. Esta asociación académica colabora con cincuenta y siete organizaciones internacionales de estudios en más de treinta países, forma parte del International Social Science Council y goza de estatus consultivo ante la Organización de las Naciones Unidas. Sus principales revistas académicas son: *Foreign Policy Analysis*, *International Political Sociology*, *International Studies Perspectives*, *International Studies Quarterly* e *International Studies Review*.

Una búsqueda de la palabra *wikileaks* en el sitio web de la International Studies Association sólo nos dio un resultado, el *call for papers* 'Power, Principles and Participation in the Global Information Age'[3], del año 2012, en el que se pregunta: "¿Cómo ha impactado la información en la relación entre los actores públicos y privados? ¿Qué sucede con la seguridad nacional en una era de Wikileaks?". Rastreando las cinco publicaciones científicas de la International Studies Association comprobamos, además, que las referencias a WikiLeaks o a cualquier documento filtrado por esta organización eran muy escasas.

En *Foreign Policy Analysis*, por ejemplo, no se encontró ni un solo artículo sobre WikiLeaks ni ninguna cita sobre los documentos secretos publicados por esta organización; sólo en *International Studies Perspectives* encontramos un artículo donde WikiLeaks es parte del título de un trabajo de investigación: 'Lost and Found: The WikiLeaks of De Facto State–Great Power Relations' (Scott Pegg y Eiki Berg, 2014). En total, en estas cinco revistas académicas, los cables diplomáticos publicados por

[3] Véase: http://www.isanet.org/Conferences/San-Diego-2012/Call (último acceso: 11 de febrero de 2015).

WikiLeaks fueron citados sólo nueve veces y en cuatro ocasiones fueron atribuidos directamente a WikiLeaks (los otros cinco artículos citan fuentes periodísticas que se basan en registros de WikiLeaks).

La búsqueda sin filtros para la palabra *wikileaks* en Wiley Online Library —una de las plataformas científicas más importantes que existen para profesores, investigadores y estudiantes universitarios— nos devolvió 1.085 resultados relacionados con esta organización, de los cuales sólo dieciocho fueron registrados entre los años 2007 y 2010 (catorce revistas y cuatro libros), esto es, desde que WikiLeaks inició sus operaciones hasta el momento en que se dio a conocer en todo el mundo con las publicaciones masivas de documentos de las guerras en Irak y Afganistán pero, sobre todo, con las filtraciones de cables de la diplomacia estadounidense. La primera referencia a WikiLeaks en esta base de datos la encontramos en el documento *Africa Research Bulletin: Economic, Financial and Technical Series*, del 8 de octubre de 2007, en concreto, en el apartado 'Kenya: Graft Report Leaked', en el que se menciona una filtración de WikiLeaks fechada el 9 de septiembre de aquel año[4], con la que hizo públicos los resultados de una investigación sobre el saqueo de los fondos de Kenia por parte del expresidente Daniel Arap Moi y sus socios, encargada en 2004 por el entonces presidente Mwai Kibaki a la empresa de inteligencia Kroll.

Entre los años 2011 y 2012, cuando iniciamos nuestra fase de exploración para esta investigación, la base de datos de Wiley Online Library recogió 336 entradas relacionadas con WikiLeaks (303 en revistas y 33 en libros), es decir, el 31 por ciento del total de los registros. Así pues, la mayor parte de los documentos registrados en Wiley Online Library con alguna referencia a WikiLeaks fueron publicados en los años 2013, 2014 y 2015, en concreto, el 67,37 por ciento (678 en revistas y 53 en libros). Y en este periodo, Wiley Online Library solamente nos devolvió en la búsqueda de la palabra *wikileaks* 97 registros en el año 2013 (78 en revistas y 19 en libros), cuando adelantamos parte de nuestra investigación, dada la emergencia del fenómeno (Quian, 2013a). En el año 2014, las publicaciones con referencias a WikiLeaks fueron 92 (73 en revistas y 19 en libros) y en 2015 cuando se produjo una explosión de la literatura con referencias a WikiLeaks, con 542 regist2ros (527 en revistas y 15 en libros). Sin embargo, en la mayoría de estos registros WikiLeaks es un elemento secundario o casi

[4] Véase: *The Looting of Kenya: Daniel Arap Moi,* en http://wikileaks-press.info/the-looting-of-kenya-daniel-arap-moi/ (último acceso: 11 de febrero de 2015).

anecdótico. Al acotar la búsqueda para la palabra *wikileaks* a títulos de publicaciones y de artículos, resúmenes y palabras clave, el buscador de Wiley Online Library sólo nos devolvió 33 resultados para el periodo 2007-2015: 25 en revistas científicas y ocho en libros. Once de estos registros fueron publicados en 2011, cinco en 2012, seis en 2013, cinco en 2014 y seis en 2015

En el Directory of Open Access Journal (DOAJ), base de datos que provee acceso abierto a revistas científicas y académicas, encontramos menos referencias. La búsqueda en bruto para el término *wikileaks* sólo arrojó 38 resultados: tres fechados en el año 2010; 18 en 2011, seis en 2012, cinco en 2013, dos en 2014 y cuatro en 2015. De éstos, 19 incluyen la palabra *wikileaks* en su título o términos clave, y 28 en resúmenes.

En una exploración en Dialnet —portal de difusión de la producción científica hispana, centrado fundamentalmente en los ámbitos de las Ciencias Humanas, Jurídicas y Sociales— sólo encontramos 121 documentos (110 artículos de revistas, nueve artículos de libros y dos libros). El primer registro es un artículo de Gonzalo Soltero titulado 'Periodismo: los golpes de WikiLeaks', publicado en el número 142 de la revista *Letras Libres*, en el año 2010.

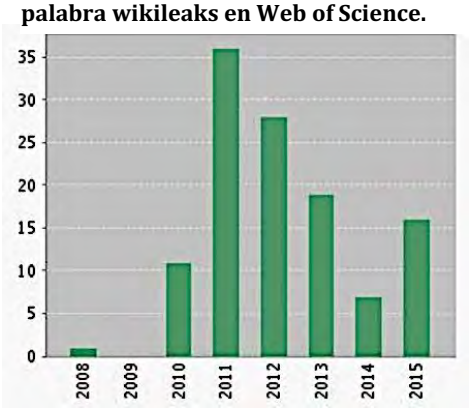
También hicimos búsquedas en las dos principales bases de datos de referencias bibliográficas y citas de publicaciones científicas internacionales: Scopus (Elsevier) y Web of Science (Thomson Reuters). Hicimos búsquedas que incluyen en su título, resumen o palabras clave el término *wikileaks*, entre los años 2007 y 2015, ambos inclusive. Estas bases de datos muestran un alto grado de solapamiento. En ambas búsquedas el primer registro histórico que se encuentra es el artículo 'Prior restraint or finger in the dike? Bank Julius Baer v. Wikileaks and Dynadot', firmado por Scott E. Graves y publicado en *Justice System Journal* en 2008. Tanto en Scopus como en la base de datos del Institute for Scientific Information no hay más referencias a WikiLeaks hasta el año 2010.

En Scopus encontramos 254 registros con la palabra *wikileaks* en su título, resumen o términos clave. De todos éstos, 143 contienen la palabra *wikileaks* en su título. Del total de referencias encontradas, 23 fueron publicadas en el año 2010, 70 en 2011, 57 en 2012, 46 en 2013, 39 en 2014 y 18 en 2015. De todos estos registros, 174 pertenecen al área de Ciencias Sociales, es decir, el 68,5 por ciento. Por tipo de documentos, se agrupan de la siguiente forma: 145 artículos, 23 ponencias, 21

revisiones, 19 capítulos de libros, once editoriales, nueve libros, nueve pequeñas encuestas, seis notas, cinco artículos en prensa y tres cartas.

En Web of Science encontramos 118 registros en una búsqueda restringida a títulos con la palabra *wikileaks*: uno en 2008, 11 en 2010, 36 en 2011, 28 en 2012, 19 en 2013, 7 en 2014 y 16 en 2015.

Gráfico 1: Registros de títulos con la palabra wikileaks en Web of Science.



Fuente: Web of Science.

En la propia Universidad Carlos III de Madrid no se ha presentado hasta el momento ninguna tesis doctoral monográfica sobre WikiLeaks, la cultura hacker y los movimientos hacktivistas, aunque sí encontramos algunas aproximaciones en algunos artículos y libros firmados por académicos de esta institución; por ejemplo, el artículo del profesor Raúl Magallón-Rosa titulado 'WikiLeaks: ¿un cambio de paradigma?', publicado en el año 2012, al que hay que sumar un par de referencias a WikiLeaks de la profesora Pilar Carrera en una parte del libro *El periodista en la encrucijada* (dirigido por la catedrática María Pilar Diezhandino), titulada 'Periodismo y social media', también en el año 2012, y otra breve referencia en el artículo 'Políticas de Estado en el modelo de prensa anglosajón', de Guadalupe Aguado-Guadalupe, Josep M. Sanmartí Roset y Raúl Magallón-Rosa, en el año 2011. La profesora de la Carlos III Susana Díaz y el catedrático de la Universidad Complutense de Madrid Jorge Lozano son los editores del libro *Vigilados: WikiLeaks o las nuevas fronteras de la información* (2013), que incluye una introducción, doce artículos de diferentes autores —incluidos los profesores Magallón y Díaz— y una entrevista con el sociólogo Alberto Abruzzese. Por su parte, el catedrático de Periodismo de la UC3M Carlos Elías ha profundizado en la cultura hacker y el fenómeno WikiLeaks en dos capítulos de sus libros *El selfie de Galileo. Software social, político e intelectual del siglo XXI* y *Big data y periodismo en la sociedad red*, ambos publicados en el año 2015, además de un articulo publicado en 2011 con el título '¿Wikileaks es periodismo ciudadano? De la ética hacker del Cablegate a la estética emo de Assange como icono global' (2011).

Por último, queremos destacar que en la base de datos de tesis doctorales del Ministerio de Educación, TESEO, no encontramos ningún trabajo monográfico sobre

WikiLeaks o hacktivismo. La búsqueda para la palabra *hacker* sí nos devolvió algunos resultados sobre trabajos públicos con aproximaciones y referencias a esta cultura. Los más recientes son: en la Universidad de Santiago de Compostela, *Cultura de red y creación estética*, de Adrián Hiebra Pardo (2013), tesis en la que el autor recurre al *ethos* de la cultura hacker para explicar un nuevo espacio discursivo para la práctica artística; en la Universitat Politècnica de València, *Comunidad y sociedad en los márgenes del diluvio tecnológico. impacto e interrupciones de las tecnologías de información y comunicación en las comunidades reales: cultura, lengua y emancipación*, de Tiago Barbedo Assis (2013), en la que reflexiona, en la primera parte de su trabajo, sobre las éticas e ideologías que dominan el concepto de lo global, incluyendo, entre otros, el ensayo de Pekka Himanen sobre ética hacker; en la Universidad Camilo José Cela, *Política 2.0 y nativos digitales: la participación de los universitarios madrileños por medio de las TIC*, de Adolfo Álvaro Martín (2012), en la se analiza, en su segundo capítulo, el debate sobre el uso de nuevas tecnologías de la información y la comunicación en política, con especial atención a la importancia de la cultura hacker en el desarrollo del ciberactivismo; y en la Universidad Autónoma de Barcelona, *The evolution of cyberpunk into postcyberpunk: the role of cognitive simulations, hive wetwares and nanotechnology in science fiction*, de Rafael Miranda Huereca (2011), en la que se describen estos géneros de ciencia ficción y se identifican algunos de sus personajes como hackers.

Antes de estos trabajos también se leyeron otras tesis con referencias a la cultura hacker: en la Universidad Politécnica de Catalunya, *Educació per a una societat de la informació sostenible*, de Marc Alier Forment (2009), en la que el autor también recurre a Himanen para explicar algunos nuevos modelos de conducta social y económica motivados por el uso de Internet y relacionados con el software y el conocimiento libres; en la Universidad Autónoma de Madrid, *Morfologías híbridas. El organismo cibernético en el cine de ciencia ficción contemporáneo* (1979-2004), de Lydia García-Merás Fernández (2009), en la que la autora describe como hacker uno de los cuatro tipos de *cyborgs* que identifica en el cine ciencia ficción; en la Universidad del País Vasco, *Prácticas y dispositivos tecno-estratégicos en la producción simbolica en red*, de Ignacion Domench Pérez (2006), en la que relaciona la cultura hacker con el arte y la respuesta a la posesión privativa del conocimiento y de la cultura; en la Universidad Complutense de Madrid, *El derecho a la intimidad en Internet*, de Marcelo Cardoso

Pereira (2006), en la que el autor incluye a los hackers en un grupo de actores que ponen en riesgo el derecho a la intimidad de los internautas, junto al Estado y a los prestadores de servicios de tecnologías de la información y la comunicación; en la Universidad Pontificia de Salamanca, *Historia de los movimientos sociales que atentan contra la seguridad informática. repercusiones sociales, políticas, éticas y psicológicas*, de Maximiliano Azorín Tobías (2005), en la que identifica a los hackers como delincuentes; y en la Universidad Pompeu Fabra, *Poder y autoridad en las relaciones internacionales: el control del comercio electrónico en Internet*, de Josep Ibáñez Muñoz (2003), en la que se hace una breve aproximación a la cultura hacker y el ciberactivismo.

Por lo tanto, podemos decir que este trabajo es pionero en España, al ser la primera tesis publicada que traza la línea evolutiva de la cultura hacker para su análisis monográfico profundo y extenso, desde sus orígenes hasta el surgimiento del hacktivismo, y la primera que estudia el fenómeno WikiLeaks, todo ello, en el contexto de la sociedad red.

Ideado como dos tesis en una, este trabajo de investigación pretende contribuir a ampliar, desde el campo de la investigación en medios de comunicación y periodismo, el estudio sobre WikiLeaks, la cultura hacker y su vertiente política.

Para realizar un estudio científico riguroso sobre el fenómeno WikiLeaks consideramos necesario aplicar un enfoque holístico que nos permitiese trazar una lógica evolutiva de seis décadas, desde la aparición de los primeros hackers computacionales en el Massachusetts Institute of Technology y de los *phone phreaks* (hackers de sistemas telefónicos), hasta la eclosión del hacktivismo informacional, del que WikiLeaks es paradigma. Entendemos que WikiLeaks es fruto del devenir hacker y que su estudio científico pierde sentido si no se aborda desde los principios y procesos evolutivos que han marcado el desarrollo de la cultura hacker, fundamental para entender además los cambios radicales comunicacionales y tecnológicos que se han producido en las sociedades modernas en las últimas seis décadas, en los que la cultura hacker ha influido de manera decisiva.

Los hackers vivieron en la más absoluta opacidad hasta el año 1984, cuando Steven Levy publicó el libro *Hackers: Heroes of the Computer Revolution*, obra fundacional de la cultura y de la ética hackers. A partir de entonces, la literatura sobre

hackers ha basculado entre los ensayos que han pretendido profundizar en los principios éticos y técnicos por los que se rigen los hackers, y el discurso penalizador amplificado por los medios de comunicación de masas y por diversos estudios sobre seguridad informática diseñados por compañías con intereses comerciales en este campo. Las primeras aproximaciones rigurosas y sustanciales sobre la cultura hacker datan de la década de 1980. Además de la obra pionera de Levy, en 1984 Sherry Turkle hace una importante contribución al conocimiento de la cultura hacker en *The Second Self: computers and the human spirit*. Ese mismo año, Stewart Brand sienta la base conceptual que marca de manera definitiva el devenir de la cultura hacker y del hacktivismo cuando en la primera Hacker Conference, en San Francisco, pronuncia el adagio que se convirtió en la razón de ser y de existir de hackers y hacktivistas: la información quiere ser libre. Tres años después, en 1987, Brand publica *The Media Lab: inventing the future at MIT*, un libro que describe la prodigiosa actividad en el Massachusetts Institute of Technology —nido hacker—, los cambios que el desarrollo de nuevas tecnologías están produciendo de manera acelerada en los medios de comunicación y sus consecuencias políticas y sociales.

Ya en 1990, Meyer y Thomas desafían la visión maniquea de los medios de comunicación de masas, que en plena efervescencia hacker contribuyen al proceso político de criminalización del hacker. En su artículo 'The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground', estos autores identifican el *ethos* antisistema que caracteriza a una cultura, la hacker, que Meyer y Thomas observan como una nueva manifestación posmodernista contra el orden económico y moral imperantes.

1990 es también el año en el que ciberlibertario John Perry Barlow publica el manifiesto *Crime and Puzzlement*, con el que se inaugura una nueva etapa que lleva a los hackers a implicarse de manera proactiva en el activismo. De este texto no sólo emerge la primera institución hacker con fines políticos de la historia, la Electronic Frontier Foundation, sino también la razón fundamental para que Bruce Sterling publique en 1992 su celebérrima obra *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, la primera exploración minuciosa sobre el conflicto político que subyace en las primeras grandes persecuciones, redadas y detenciones de hackers, y en el estrangulamiento de sus medios de comunicación, lo que contribuyó definitivamente a crear el caldo de cultivo para la resistencia y la desobediencia civil electrónicas.

Entre los medios editados por los propios hackers sobresale uno por encima de todos, la revista *2600: The Hacker Quarterly*, nacida en 1984. En el año 2009, con motivo de su veinticinco aniversario, su editor, el hacker Eric Gordon Corley —más conocido por su seudónimo Emmanuel Goldstein— articula el mayor tratado hacker jamás publicado: *The Best of 2600: A Hacker Odyssey*, una obra magna de enorme valor para cualquier investigador que quiera abordar la cultura hacker, tanto desde una perspectiva puramente técnica como desde enfoques mediológicos o políticos. *The Best of 2600: A Hacker Odyssey* es la mayor fuente documental primaria que existe sobre técnicas de *hacking*, cultura hacker y los orígenes del hacktivismo; una obra enciclopédica de 871 páginas ineludible para quien quiera estudiar el fenómeno hacker, pero también el desarrollo de la computación, de las redes móviles e inalámbricas, y de Internet.

También imprescindible es la producción literaria del hacker anarcocapitalista Eric S. Raymond, principalmente su trabajo lexicográfico en el Jargon File —el diccionario de la cultura hacker— y su ensayo *The Cathedral and the Bazaar*, en el que confronta el modelo de producción de software privativo con el del software de código abierto sobre el que descansa un principio fundamental de la comunidad hacker como es el de la libre información. El movimiento del software libre, que se considera inaugurado cuando Richard Stallman pone en marcha la Free Software Foundation en 1985, es la materialización del ideal hacker y hacktivista de la libre información. Algunas de las propuestas más radicales sobre el software libre se hallan en la literatura del profesor de Derecho e Historia en la Universidad de Columbia Eben Moglen, autor del *dotCommunist Manifesto* (2003) y de los artículos 'Anarchism Triumphant: Free Software and the Death of Copyright' (1999) y 'Freeing the Mind: Free Software and the Death of Proprietary Culture' (2003).

El movimiento del software libre contribuye, junto con el desarrollo de las primeras comunidades red en Internet y la eclosión del ciberespacio, a que una retórica ciberanarquista y ciberlibertaria, articulada por algunas elites de hackers, vaya impregnando de radicalismo político el ambiente en el *underground* computacional desde principios de la década de 1990. Fundamental es la aparición en 1992 de la lista de correo electrónico *Cypherpunks*, una comunidad de criptoanarquistas cuyos fundamentos políticos asienta Timothy C. May en 1994 en el *Cyphernomicon.* Es de esta lista de correo de donde se nutre el pensamiento político de Julian Assange,

actualizado e impreso en el año 2012 en el libro *Cypherpunks*, en un diálogo con los hacktivistas y *cypherpunks* Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann, que pretende revitalizar la retórica ciberlibertaria, también recuperada por Adam Thierer y Berin Szoka en su artículo 'Cyber-Libertarianism: The Case for Real Internet Freedom' (2009).

En el contexto del cambio de paradigma que supone la eclosión del ciberespacio y de las redes electrónicas de comunicación, y en pleno fulgor hacker, un nuevo enfoque militarista sobre los flujos de información en la Red empieza a consolidarse desde principios de la década de 1990 a partir de las investigaciones y análisis de Arquilla y Ronfeldt para el laboratorio de ideas RAND Corporaton, que provee servicios a las Fuerzas Armadas de Estados Unidos. Su trabajo es fundamental para comprender la disputa que hoy se libra por la información, que se ha convertido en el principal conflicto de nuestros tiempos. Arquilla y Ronfeldt acuñan los conceptos *netwar* y *cyberwar*, y desarrollan toda una teoría sobre las guerras de la información que ha influido de manera decisiva en el desarrollo conceptual y práctico de los conflictos informacionales. Su artículo 'Cyberwar Is Coming!' (1993) y sus libros *The Emergence of Noopolitik: Toward an American Information Strategy* (1999) y *Networks and netwars: The Future of Terror, Crime and Militancy* (2001) asientan las bases de una nueva era en la que, como nunca antes, se evidencia que la información es poder.

Son precisamente las teorizaciones de Arquilla y Ronfeldt las que empujan definitivamente a muchos hackers al activismo político y a un sector del activismo político tradicional, al empleo de técnicas hacker. La base teórica para el desarrollo del hacktivismo se halla fundamentalmente en el seno del grupo activista Electronic Disturbance Theater y del colectivo hacker Cult of the Dead Cow. Bajo el paraguas del primero, el teórico Stefan Wray articula los ejes teóricos para la desobediencia civil electrónica en respuesta a los textos de Arquilla y Ronfeldt, principalmente en sus artículos 'Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics' (1998) y 'On Electronic Civil Disobedience' (1999), textos que influyen en trabajos como el de Mark Manion y Abby Goodrum en 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' (2000). A la par, Oxblood Ruffin, hacker de Cult of the Dead Cow, es el primero en desarrollar una definición de hacktivismo y el primer teórico que vincula el desarrollo de herramientas y técnicas hackers a la defensa de los principios recogidos en la

Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. Su *paper* 'Hacktivism, From Here to There', presentado en el año 2004 en la Facultad de Derecho de Yale, en el marco de la CyberCrime and Digital Law Enforcement Conference, es una de las principales referencias a las que todo investigador debe recurrir para abordar el activismo hacker.

Tim Jordan y Paul Taylor son los autores más prolíficos en la investigación sobre hacktivismo. Sus trabajos, desde 1999, trazan buena parte de las principales líneas a seguir en el estudio del activismo hacker, primordialmente su libro *Hacktivism and Cyberwars: Rebels with a cause?* (2004). También tesis doctorales tempranas sobre activismo hacker como *Hacking for Democracy: A Study of the Internet as a Political Force and Its Representation in the Mainstream Media* (Sandor Vegh, 2003) y *Hacktivism and the Future of Political Participation* (Alexandra Whitney Samuel, 2004) son pioneras al abrir líneas de investigación nuevas sobre hacktivismo.

La convergencia de todos estos movimientos y fenómenos, de la que brota WikiLeaks, es difícil de explicar si no se enmarca en el informacionalismo, el paradigma tecnológico que está sustituyendo y subsumiendo al industrialismo como matriz dominante de las sociedades del siglo XXI, y que proporciona la base para un nuevo tipo de estructura social que el profesor Manuel Castells (1997, 2001a, 2001b, 2006, 2009) denomina sociedad red, en la que Internet es ya el medio de comunicación y de relación esencial sobre el que se basa esta nueva forma de sociedad. Pero es Pekka Himanen (2001) quien por primera vez identifica en la ética hacker el espíritu alternativo del informacionalismo frente a la lógica de las redes económicas formulada por Castells en *La era de la información* (1997). Himamen es quien propone por primera vez la idea de una nueva empresa u organización red con unos valores éticos distintos a los dominantes en la sociedad red, en la que las empresas y los Estados-red se gobiernan con valores puramente instrumentales para alcanzar metas económicas. Frente a los valores del capitalismo tecnológico excluyente en el que se asienta la sociedad red, Himanen aboga por la ética hacker como desafío de una preocupación responsable en plena era de la información.

Tras la eclosión de WikiLeaks y la consolidación de un nuevo modelo de organización red en la que se funden hacktivismo y periodismo, se hace necesario revisar y actualizar toda esta literatura e iniciar nuevas líneas de investigación que

completen este poliedro informacional, para abordar el impacto de un fenómeno como WikiLeaks en los medios de comunicación, en la política internacional, regional y local, y en la opinión pública. Siguiendo el planteamiento de Walter Lippmann en *La opinión pública* ([1922] 2003:53), parece oportuno preguntarse ahora por qué medios se han llegado a conocer los hechos sobre WikiLeaks en los que se han basado la opiniones sobre este fenómeno, pero también, y sobre todo, cuándo y cómo este fenómeno impactó en la opinión pública, para dilucidar la estrategia diseñada en el seno de esta organización.

4. ESTRUCTURA DEL TRABAJO

Este trabajo ha sido estructurado de tal manera que nos permita seguir una lógica metodológica y argumentativa.

Los capítulos I y II aportan la base teórica, conceptual, histórica y crítica para nuestro estudio de caso, siguiendo un razonamiento evolutivo que nos lleva desde la génesis hacker y su impacto mediático y social, hasta la eclosión del hacktvismo como manifestación política de la ética hacker y su impacto en la sociedad red.

El capítulo III contiene una crítica analítica del marco contextual en el que se desarrolla la sociedad red en Internet, de los nuevos mecanismos de interacción entre medios de comunicación y ciudadanos, y de los modelos periodísticos que brotan de las emergencias informacionales.

El capítulo IV se dedica a nuestro caso de estudio, WikiLeaks, el cual abordamos primero desde un enfoque teórico-conceptual e histórico que continúa la línea narrativa y completa la argumentación de los capítulos precedentes, para continuar luego con una descripción analítica y crítica del fenómeno WikiLeaks y, finalmente, someterlo al escrutinio empírico del que se derivan nuestras conclusiones, que acompañamos con unas valoraciones finales y una serie de recomendaciones.

Las referencias de las fuentes documentales utilizadas y un conjunto de anexos con información complementaria sobre el trabajo de investigación completan esta tesis.

5. METODOLOGÍA

5.1. Integración de métodos cualitativos y cuantitativos

Para abordar el caso de estudio que nos ocupa consideramos que era necesario integrar métodos cuantitativos y cualitativos, separados y confrontados en el pasado en la investigación científica que busca averiguar, descifrar, comprender, resolver y/o formular nuevos problemas y fenómenos que afectan al ser humano como individuo social y como especie animal, (inter)conectado con sus artificios, con otros seres vivos y con su entorno natural y artificial. Vamos a justificar aquí la necesidad de integrar métodos cualitativos y cuantitativos en nuestro estudio.

5.1.1. Breve aproximación a los conceptos cualitativo/cuantitativo

Según el diccionario de la Real Academia Española de la Lengua, lo cualitativo "denota cualidad" y la cualidad se refiere a "cada uno de los caracteres, naturales o adquiridos, que distinguen a las personas, a los seres vivos en general o a las cosas", y la "manera de ser de alguien o algo". Por otra parte, define así lo cuantitativo: "Perteneciente o relativo a la cantidad". Y la cantidad hace referencia a una "porción de una magnitud", a un "cierto número de unidades", a una "porción grande o abundancia de algo" y a un "número que resulta de una medida u operación". *Cualidad*, además, comparte con *calidad* su raíz latina, pues ambas palabras proceden del latín *qualitas*, que deriva de *qualis* (cuál, qué). Para Aristóteles, "la cualidad es la diferencia o característica que distingue una sustancia o esencia de las otras", y "la forma sintética de la cualidad no puede reducirse a sus elementos sino que pertenece esencialmente al individuo y es la que hace que éste sea tal o cual" (Martínez Miguélez, 2006: 127). Es esta acepción, en sentido propio, filosófico, la que se usa en el concepto de metodología cualitativa:

> De esta manera, la investigación cualitativa trata de identificar la naturaleza profunda de las realidades, su sistema de relaciones, su estructura dinámica, aquella que da razón plena de su comportamiento y manifestaciones. De aquí, que lo cualitativo (que es el todo integrado) no se opone a lo cuantitativo (que es sólo un aspecto), sino que lo implica e integra, especialmente donde sea importante (Martínez Miguélez, 2006: 128).

La dicotomía entre cualitativo y cuantitativo es, por tanto, un falso dilema (Landreani, 1990) que ha dado lugar en las Ciencias Sociales a tres posturas: la cualitativista, la cuantitativista —enfrentadas, aparentemente irreconciliables— y una complementaria entre ambas (Jick, 1979). Como explican Cook y Reichardt (1986), el conglomerado de atributos que integran el paradigma cuantitativo procede de las Ciencias Naturales y Agronómicas, mientras que el paradigma cualitativo tiene su origen en la Antropología Social y la Sociología, especialmente en la Escuela de Chicago. El paradigma cuantitativo se construyó sobre la concepción global positivista, hipotético-deductiva, particularista, objetiva, orientada a los resultados y propia de las Ciencias Naturales, y se empezó a aplicar en Ciencias Sociales a finales del siglo XIX y comienzos del XX. Por su parte, el paradigma cualitativo se sustentó en una concepción global fenomenológica, inductiva, estructuralista, subjetiva, orientada al proceso y propia de la Antropología Social (Cook y Reichardt, 1986; Mokate, 2003).

Cuadro 2: Atributos de los paradigmas cualitativo y cuantitativo.

Paradigma cualitativo	Paradigma cuantitativo
Aboga por el empleo de los métodos cualitativos.	Aboga por el empleo de los métodos cuantitativos.
Fenomenologismo y *verstehen* (comprensión) "interesado en *comprender* la conducta humana desde el propio marco de referencia de quien actúa".*	Positivismo lógico; "busca los *hechos* o *causas* de los fenómenos sociales, prestando escasa atención a los estados subjetivos de los individuos".*
Observación naturalista y sin control.	Medición penetrante y controlada
Subjetivo.	Objetivo.
Próximo a los datos; perspectiva "desde dentro".	Al margen de los datos; perspectiva "desde fuera".
Fundamentado en la realidad, orientado a los descubrimientos, exploratorio, expansionista, descriptivo e inductivo.	No fundamentado en la realidad, orientado a la comprobación, confirmatorio, reduccionista, inferencial e hipotético deductivo.
Orientado al proceso.	Orientado al resultado.
Válido: datos "reales", "ricos" y "profundos".	Fiable: datos "sólidos" y repetibles.
No generalizable: estudios de casos aislados.	Generalizable: estudios de casos múltiples.
Holista.	Particularista.
Asume una realidad dinámica.	Asume una realidad estable

Fuente: Cook y Reichardt (1986: 29).

En un sentido fundamental, los métodos cualitativos pueden ser definidos como técnicas de comprensión personal, de sentido común y de introspección, mientras que los métodos cuantitativos podrían ser definidos como técnicas de contar, de medir y de razonamiento abstracto (Cook y Reichardt, 1986)

Pero a pesar de estos atributos aparentemente opuestos y contradictorios, para Kenneth Howe (1988: 12) "lejos de ser incompatibles, los métodos cuantitativos y cualitativos están inextricablemente entrelazados". Así, descarta la teoría de incompatibilidad y propone la teoría de compatibilidad que aboga por la combinación de ambos enfoques. Para ello, Howe examina los cuatro componentes básicos de investigación: datos, diseño, análisis e interpretación. Y si bien en el nivel de los datos la distinción cuantitativa-cualitativa es ambigua, al nivel de diseño, análisis e interpretación, los elementos cuantitativos (mecánicos y estables) y los cualitativos (no mecánicos y dinámicos) son interdependientes e inseparables. Es decir, para Howe resulta imposible un estudio sin elementos cualitativos en el diseño, análisis e interpretación, ya que son esos elementos que caracterizan y definen la exploración cuantitativa (Mokate, 2003).

Así pues, a pesar de esta aparente antítesis o dicotomía que se predicó en el pasado, se da una imposibilidad epistémica de separar lo cuantificable de lo cualificable, pues toda medición se realiza para descifrar las cualidades del objeto de estudio. Pero esa imposibilidad de la antítesis o dicotomía entre cantidad y cualidad surge también en la imposibilidad de separar la intervención del sujeto investigador del objeto de estudio, especialmente en las Ciencias Sociales, en las que es más evidente que el que mide toma para sí, interviene, sesga y modifica lo medido.

> No hay realidades cuantitativas, ni realidades cualitativas, o, si se prefiere, caracteres cuantitativos o atributos cualitativos inherentes de los objetos. No las hay, simplemente, porque no existen objetos externos, preexistentes e independientes del sujeto observador. Es el sujeto, sea o no investigador social, el que define las propiedades cuantitativas o cualitativas de los objetos (Montañés Serrano, 2007: 15).

Si la objetividad es un rasgo definitorio del enfoque cualitativo y la subjetividad lo es del cualitativo, las líneas fronterizas entre uno y otro se vuelven extremadamente delgadas e incluso se puede decir que se diluyen en las Ciencias Sociales, donde la experiencia, los juicios, las opiniones, el entorno y la condición

humana del observador determinan decisivamente el estudio del objeto. Así, Cook y Reichardt, por su parte, se preguntan si son necesariamente subjetivos los procedimientos cualitativos y necesariamente objetivos los procedimientos cuantitativos. En su opinión, todos los métodos y medidas, tanto cualitativos como cuantitativos, son subjetivos, es decir, están influidos por el juicio humano:

> Desde luego, los modernos filósofos de la ciencia coinciden en gran parte en señalar que todos los hechos se hallan inspirados por la teoría y así resultan, al menos parcialmente, subjetivos. Por supuesto que la asignación de números de una manera mecánica, como es común en los procedimientos cuantitativos, no garantiza la objetividad (Cook y Reichardt, 1986: 32).

Sin duda, el sesgo del investigador y su arbitrariedad intervienen en su aproximación al problema y al objeto de estudio e imprimen cualidad a cualquier análisis cuantitativo al que se enfrente, de modo que la pretendida objetividad es parcial y limitada, y el dato obtenido, fragmentario y condicionado. Esto se manifiesta, por ejemplo, en cualquier cuestionario diseñado por el investigador, que es quien determina, en función de criterios subjetivos, las variables utilizadas, las preguntas y las opciones de respuesta que limitan y condicionan al encuestado, cuyas respuestas serán codificadas y cuantificadas para facilitar una posterior interpretación y comprensión y, por lo tanto, obtener cualidades de los datos cuantificados.

Así, tanto en los trabajos de carácter distributivo (cuantitativo) como estructurales (cualitativo) la finalidad y los objetivos de la investigación están fijados previamente por un sujeto trascendente. "Ambas técnicas están al servicio de un cliente que actúa como sujeto trascendente, que es quien construye el cuento" (Montañés Serrano, 2007: 16).

Resulta de especial interés la observación de Montañés Serrano, para quien no hay inherentes realidades cuantitativas o cualitativas, sino que tales características dependen del sujeto observador. De modo que en cualquier enfoque cuantitativo todo depende de los cuentos con los que poder hacer cuentas:

> […] para hacer cuentas previamente se ha de contar cuentos con los que establecer identidades y diferencias.
>
> Quien aplica una encuesta, u otro tipo de dispositivos distributivo, obvia la existencia del cuento de partida, o procede como si todas las personas, que a la misma contestan, hubiesen partido del mismo cuento y otorgasen en mismo significado al reificado significante resultante de la operación efectuada. No tiene en cuenta, en definitiva, la polisemia de todo significante (Montañés Serrano, 2007: 16).

Además, el dato cuantitativo, el número, la cantidad, al ser parte de un todo integrado variable, cuestiona su valor estable y es susceptible de ser voluble y mutable, y, por lo tanto, adquiere las cualidades variables y dinámicas de la vida y de la actividad humana.

Así pues, se hace necesario tomar conciencia de que los fenómenos sociales, o los impactos o efectos sociales, tienen dimensiones tanto cuantitativas como cualitativas indisolubles. Sólo así, tomando conciencia de que la cantidad imprime cualidad y la cualidad se forja también en la cantidad, podemos superar la brecha entre lo cualitativo y lo cuantitativo (Mokate, 2003)

5.1.2. La indisolubilidad de lo cualitativo y lo cuantitativo

Jesús Ibáñez (1988) inscribe tanto las técnicas cuantitativas como las cualitativas en procesos de *matematización* del orden social, es decir, del análisis ordenado del orden. Por eso juzga innecesaria la distinción cuantitativo *vs* cualitativo, pues la *matematización* se aplica al análisis del orden social y no únicamente del orden numérico.

La disyuntiva epistemológica entre estos dos conceptos en las Ciencias Sociales fue en realidad una disyuntiva semántica o lingüístico-semiótica que infectó a los modos de enfocar la obtención y análisis de información a través del método científico. Ninguna técnica cuantitativa en el campo de las Ciencias Sociales se explica sin un aporte de cualidad, pues el número, la magnitud, la extensión, la cantidad, no adquiere sentido sin su interpretación y comprensión y, por tanto, sin una aplicación cualitativa. Siguiendo la lógica *hegeliana*, todo dato cuantitativo requiere de una explicación que le otorgue un significado; así, la cantidad deriva en cualidad, y viceversa.

El conocimiento cualitativo y el conocimiento cuantitativo se retroalimentan, de modo que el primero puede beneficiarse del segundo: un hallazgo cuantitativo puede estimular una ulterior indagación cualitativa (Light, 1979; Sieber, 1973); de igual modo, los investigadores cualitativistas no pueden prescindir del hecho de contar elementos o de emplear conceptos cuantitativos como “más grande que” y “menos que” (Cook y Reichardt, 1986).

Pensar que la naturaleza humana se reduce básica y esencialmente al número, a la pura cuantificación, sería reducir la condición humana a una abstracción y estabilidad que contradice el dinamismo humano. Y a la vez, los cambios generados por las iniciativas sociales, no por ser intangibles y dinámicos resultan ser no medibles o no verificables; todo lo contrario. Por ejemplo, en los resultados de unas elecciones presidenciales, el número de votos y los porcentajes obtenidos por cada candidatura no son sólo meros datos cuantitativos, puras abstracciones matemáticas, sino que cualifican a la sociedad en las que se activan los comicios, contribuyendo a interpretarla, comprenderla, evaluarla e identificarla como de izquierdas o de derechas, progresista o conservadora. De igual modo, una encuesta estadística es una técnica cuantitativa-cualitativa, pues la acumulación de datos tiene como finalidad identificar, describir, explicar y detallar las cualidades del grupo objeto de estudio. Al mismo tiempo, unos comicios o una encuesta medirán, por comparación, los cambios cualitativos producidos en un colectivo humano.

5.1.3. Conclusión

Superar el debate reduccionista sobre lo cuantitativo y lo cualitativo fue un reto fundamental para las Ciencias Sociales, para aproximarse a realidades evaluables, en cuanto a medibles y cualificables. Es por ello que el conocimiento cuantitativo debe basarse en el conocimiento cualitativo, y viceversa, ya que toda comprensión cuantitativa presupone un conocimiento cualitativo y toda medición se halla fundada en suposiciones cualitativas del observador acerca de la naturaleza del instrumento de medida y de la realidad evaluada. “Muy simplemente, los investigadores no pueden beneficiarse del empleo de los números si no conocen, en términos de sentido común, lo que éstos significan” (Cook y Reichardt, 1986: 46). Así, lejos de ser antagónicos, los dos tipos de conocimientos resultan complementarios y se necesitan mutuamente, ya que ninguno de los dos puede proporcionar por sí solo la profundidad de percepción, o visión binocular, que alcanzan conjuntamente (Eisner, 1977).

Igartua y Humanes (2004) proponen un paradigma integrador, triangulado, para obtener un más profundo conocimiento en la investigación de una realidad, donde se entrecruzan y deben converger datos de distintas fuentes, equipos interdisciplinares, perspectivas de análisis y métodos de investigación. En definitiva, su propuesta es

superar la dicotomía entre métodos cuantitativos y cualitativos, aplicando el paradigma triangulado (aplicación de distintas metodologías en el análisis de una misma realidad) para obtener un conocimiento más ajustado del objeto de estudio.

Como bien advierten Cook y Reichardt (1986), la conceptualización de los tipos de métodos como antagónicos podría llevar por mal camino nuestra práctica metodológica.

5.2. Un modelo de metodología múltiple

5.2.1. Introducción

Para abordar nuestra investigación consideramos necesario integrar enfoques cualitativos y cuantitativos en una metodología múltiple y coherente, en la que los paradigmas positivistas y hermenéuticos no fuesen excluyentes, sino compatibles. Una vez asumido que ningún método de investigación se ha mostrado superior a otro en el campo de las Ciencias Sociales (Denzin, 1970), nuestro propósito, desde un principio, ha sido aplicar la triangulación como estrategia de investigación, considerando que cuanto mayor fuese la variedad de métodos y técnicas compatibles empleadas, aplicados de manera coherente, es decir, de forma que nos permitiesen lograr hallazgos complementarios, mayor sería la fiabilidad y precisión de la investigación de un objeto poliédrico como WikiLeaks.

El uso de técnicas de triangulación ha sido ampliamente defendido como estrategia válida y recomendable en la investigación social (Jick, 1979). Por ejemplo, Smith (1975) señala que las proposiciones confirmadas por un solo método pueden tener un grado de validez menor que aquellas que sobreviven a la confrontación de distintas metodologías. Es más, autores como Oppermann (2000) se atreven a asegurar que la utilización de un único método o enfoque de investigación corre más riesgos de incurrir en sesgos.

Abordar un objeto de estudio tan complejo como WikiLeaks requería, por lo tanto, una diversidad de métodos, técnicas e instrumentos aplicados para reflejar su complejidad, procurar una mayor validez de los resultados y mitigar los ineluctables problemas de sesgo (Blaikie, 1991).

Pasamos ahora a describir detalladamente nuestra metodología.

5.2.2. Enfoque teórico-crítico

A partir de la revisión de la producción científica, literaria y periodística, y en el marco del paradigma informacional del que brota la sociedad red, nuestra investigación arma un análisis teórico-conceptual, histórico referencial, interpretativo y crítico que se desarrolla, como ya hemos visto, en el primer capítulo, dedicado a la ética y cultura hackers de las que es heredera WikiLeaks; en el segundo capítulo, centrado en el hacktivismo como manifestación política del *hacking*, y en el tercer capítulo, donde desarrollamos el análisis crítico del ecosistema informacional que domina la Red. Nuestro camino teórico-crítico prosigue en el capítulo cuarto —donde abordamos nuestro caso de estudio— con la descripción analítica del fenómeno WikiLeaks, incluyendo la revisión de los principios *cypherpunks* como base teórica del pensamiento de Julian Assange, la configuración de WikiLeaks como organización red, la evolución de su estrategia de difusión informativa y de su relación con los medios de información de masas, y el análisis de estrategias de *storytelling* aplicadas por los principales actores en el debate público sobre WikiLeaks —principalmente, políticos, medios de comunicación, grupos de apoyo a WikiLeaks y el propio Julian Assange—, y del fenómeno transmediático que han originado WikiLeaks y Julian Assange.

Los principales pilares documentales sobre los que sostenemos este trabajo son: *The Best of 2600: A Hacker Odyssey* (Goldstein, 2009), *The Hacker Ethic and the Spirit of the Information Age* (Himanen, 2001), *Hacktivism and Cyberwars: Rebels with a cause?* (Jordan y Taylor, 2004), *Cypherpunks* (Assange *et al.*, 2012), así como los ensayos teóricos de Arquilla y Ronfeldt sobre las guerras de la información (1993, 1999, 2001), las teorizaciones de Wray (1998, 1999) y de Ruffin (2004) sobre desobediencia civil electrónica y hacktivismo, y el ensayo político de Assange *Conspiracy as Governance* (2006). Las aportaciones fundamentales de Levy (1984) sobre la ética y cultura hackers, las de Sterling (1992) sobre los primeros grandes encontronazos de los hackers con los poderes institucionales, y las de Castells (1997, 2001a, 2001b, 2006, 2009) sobre la sociedad red, son los refuerzos fundamentales de estos pilares, junto con la necesaria revisión de otras fuentes científicas, ensayísticas y periodísticas para el análisis del impacto mediático y sociopolítico de la cultura hacker y del hacktivismo, en general, y de WikiLeaks, en particular.

Nuestra intención es explorar las principales fuentes documentales sobre *hacking* y hacktivismo que existen y trasladar al ámbito de la investigación en español algunos de los textos más sustanciales que sobre estos fenómenos se han publicado en inglés y de los cuales, en algunos casos, inéditos en lengua española. Principalmente, *The Best of 2600: A Hacker Odyssey*, el mayor tratado sobre cultura y técnicas hackers publicado hasta ahora, pero también un relato fundamental para quien quiera comprender el origen y los años más decisivos en el desarrollo de nuestra sociedad digitalizada y en red. Este libro es la fuente fundamental en nuestra investigación para arrojar luz sobre la comunidad hacker desde el enfoque de la investigación en medios de comunicación. Por eso, son numerosas las referencias que en esta tesis hacemos a esta magna obra de 871 páginas editada por Emmanuel Goldstein, que abarca los veinticinco años más intensos y decisivos en el desarrollo de la cultura hacker y de Internet. Nuestra intención es facilitar a los investigadores hispanos el acceso a una obra fundamental para comprender el mundo hacker desde dentro del propio mundo hacker.

También son numerosas en esta tesis las citas y referencias a documentos históricos de la cultura hacker y del movimiento hacktivista que existen aún, casi todos en inglés, muchos disponibles en *escondrijos* de la Red, escasamente difundidos, y que corren riesgo de desaparecer en un entorno, Internet, donde todo es líquido, donde abundan los enlaces rotos a páginas web que una vez mostraron contenidos y ahora devuelven páginas de error, o a sitios web completamente aniquilados. La conservación de la información y del conocimiento en la era digital se presenta como uno de los grandes retos que tenemos por delante. Porque podríamos estar cultivando el ocaso de una civilización que podría estar dirigiéndose hacia un precipicio de desmemoria, hacia un agujero negro de desconocimiento si no se asegura la conservación de todo el conocimiento y de los relatos históricos que se vierten en la Red. ¿Dónde estará dentro de un sigo todo el conocimiento que científicos comparten en espacios personales o colaborativos en la Web? ¿Dónde estarán los documentos en línea que hemos recuperado para esta tesis? ¿Dónde están los que se han perdido ya en Internet? El autor de esta tesis no puede asegurar hoy que dentro de cinco, diez, veinte, cincuenta o cien años todos los contenidos electrónicos referenciados en este trabajo se puedan encontrar en las URL aportadas aquí, ni siquiera en todo Internet. En nuestro propio trabajo de investigación hemos experimentado estos problemas, trabajando con

herramientas en línea de analítica web que luego desaparecieron, o intentando acceder a trabajos referenciados en documentos con enlaces electrónicos rotos, ya sea porque su URL original había sido modificada o porque el contenido ya no existía.

Es necesario, por tanto, que consideremos la necesidad de desarrollar y poner en marcha procesos y sistemas de protección y de conservación, en distintos soportes y formatos, de los datos, de las informaciones, de los contenidos científicos y culturales, y de todo cuanto configure nuestra historia, nuestra memoria, nuestro conocimiento y metarrelato de nuestra sociedad. Por eso hacemos nuestra la advertencia que George Orwell lanzó en su novela *1984*: "El pasado es únicamente lo que digan los testimonios escritos y la memoria humana".

Con la recuperación y traducción al español de documentos históricos de la cultura hacker y de su vertiente hacktivista, buscamos confrontar los discursos de los medios de masas con los propios de la cultura hacker y contribuir al conocimiento de los momentos y de los actores más decisivos en la historia del *hacking* y del hacktivismo. Pero también es nuestro interés, desde el ámbito académico, colaborar en su preservación como archivos históricos, como antes han hecho, por ejemplo, la revista *2600*, el Electronic Privacy Information Center (EPIC) o el colectivo internacional The Thing, gracias a los cuales pudimos acceder, por ejemplo, a una copia de los contenidos que una vez publicó en Internet el grupo ciberactivista Electronic Disturbance Theater, o a los arhivos de *Computer Underground Digest*, un boletín de noticias electrónico de periodicidad semanal, editado entre marzo de 1990 y marzo de 2000 por dos profesores de Derecho Penal en la Northern Illinois University, Gordon Meyer y Jim Thomas, interesados en los aspectos sociales y jurídicos derivados del auge de las telecomunicaciones y de Internet.

Pero estos y otros repositorios en línea podrían desaparecer algún día. Lo mismo sucede con los sitios web del grupo hacker Cult of the Dead Cow, del proyecto Hacktivismo o de la lista *Cypherpunks*, cuya existencia no está asegurada en el futuro. Estos son sólo algunos ejemplos de los materiales que utilizamos en esta tesis —algunos, inéditos en español— con la intención de describir y analizar los momentos más decisivos de la cultura hacker y del hacktivismo, facilitar su comprensión en español y contribuir, desde el ámbito académico, a su conservación como documentos históricos, incluida la reproducción íntegra de algunos manifiestos hackers.

5.2.3. Entrevista a Richard Stallman

Para enriquecer las consideraciones teóricas y el análisis crítico expuestos a partir de la revisión documental nos pusimos como objetivo prioritario entrevistar a Julian Assange. Para ello, contactamos con el equipo de WikiLeaks en su dirección de correo electrónico *sunshinepress@this.is*. Lamentablemente, nuestras gestiones no tuvieron el éxito deseado. Sin embargo, nos surgió la oportunidad de entrevistar a Richard Stallman, considerado el último hacker del Massachusetts Institute of Technology (más conocido como MIT) —la cuna de la cultura hacker—, fundador de la Free Software Foundation, gurú del movimiento mundial por el software libre y el *copyleft*[5] —antítesis del *copyright*—, y padre del proyecto GNU para el desarrollo de un sistema operativo completamente libre. Y no la desaprovechamos.

Contar con una fuente primaria de tal categoría supuso para nosotros un enorme aliciente, ya que nos permitía introducir en nuestro trabajo el testimonio y la opinión de primera mano de quien ha sido considerado en las tres últimas décadas la voz más respetada en el mundo hacker. La entrevista se acordó mediante un intercambio de correos electrónicos, se hizo por teléfono y su contenido lo adelantamos en el periódico digital *Galicia Confidencial* (Quian, 2013c), uno de los pocos sitios web en España que creó un *mirror*[6] (web espejo) de la página oficial de WikiLeaks, en pleno acoso político y bloqueo económico a esta organización, para garantizar que sus contenidos fuesen accesibles en caso de que el sitio de WikiLeaks fuese inutilizado.

La entrevista, semiestructurada, fue diseñada para:

- Dilucidar qué es ser hacker y qué es el *hacking*.
- Abordar la dimensión ética y política del *hacking*.
- Esclarecer el papel que han jugado los medios de comunicación de masas y los medios y redes sociales en línea para la comprensión social del *hacking*.

[5] La Fundación Copyleft se refiere a este neologismo anglosajón como un grupo de licencias cuyo objetivo es garantizar que cada persona que recibe una copia de una obra pueda a su vez usar, modificar y redistribuir el propio trabajo y las versiones derivadas del mismo. Unas veces se permite el uso comercial de dichos trabajos y en otras ocasiones no, dependiendo de qué derechos quiera ceder el autor.

[6] En Internet, un espejo (del inglés *mirror*), es un sitio web que contiene una réplica exacta de otro. Se suelen crear para facilitar grandes descargas y el acceso a la información aun cuando haya fallos en el servicio del servidor principal.

- Identificar las esencias hackers de WikiLeaks y de grupos hacktivistas como Anonymous.
- Juzgar la importancia del software libre, de la privacidad y de la transparencia informativa como pilares democráticos.
- Valorar el nivel de democracia y de libertad en la era de la sociedad red.

Las aportaciones de Stallman son introducidas en los diferentes capítulos de este trabajo para completar nuestro enfoque teórico-crítico.

5.2..4. Lingüística computacional aplicada al análisis del discurso sobre WikiLeaks

Para nuestro caso de estudio aplicamos un análisis de contenido cualitativo-cuantitativo de los discursos armados en las redacciones de los medios colaboradores de WikiLeaks en el *Cablegate*, centrándonos en los relatos de *The New York Times*, *The Guardian* y *El País*, tres de los cinco medios seleccionados por WikiLeaks para publicar los cables diplomáticos de Estados Unidos. *The Guardian* y *The New York Times* fueron los periódicos que negociaron, lideraron y marcaron las pautas de la cobertura informativa del *Cablegate*, además de publicar dos libros editados a finales de enero de 2011 que recogen las experiencias de sus periodistas con WikiLeaks. Por su parte, el diario español *El País* fue el periódico elegido para impactar a la opinión pública hispanohablante. Nuestra intención es describir y analizar el relato de los hechos que llevaron a WikiLeaks y a estos periódicos a romper sus vínculos de manera abrupta, tras mantener una estrecha relación. Para ello, nuestra capacidad humana de interpretar los hechos y los textos es ampliada con la computación lingüística. En concreto, nos valemos de Linguakit, un paquete de herramientas lingüísticas y de extracción textual desarrollado por Cilenis Language Technology (2014), *spin-off* de la Universidade de Santiago de Compostela.

El desarrollo de la computación, de la inteligencia artificial y del *big data* (acumulación y procesamiento de grandes volúmenes de datos), combinados con la lingüística, están revolucionando la manera en la que aprehendemos y usamos el lenguaje natural. Los traductores y correctores automáticos o los diccionarios en línea

son sólo parte del nuevo escenario en el procesamiento de lenguajes naturales y del desarrollo de la inteligencia lingüística.

La lingüística computacional está avanzando a pasos agigantados y es una de las áreas en las que más están invirtiendo los titanes del software y de la comunicación en línea, como Google o Microsoft. En un terreno más local, pero no por ello menos innovador y sustancial, encontramos nuevas empresas como Cilenis, que trabaja en el desarrollo de herramientas avanzadas en áreas de procesamiento y análisis del lenguaje natural y extracción de información, para hacer nuestras comunicaciones más fáciles y nuestro uso y comprensión de la lengua, mejores.

Cilenis nació en el año 2011 en el CiTIUS, el Centro Singular de Investigación en Tecnologías de la Información de la Universidade de Santiago de Compostela. Su principal proyecto es Linguakit, un paquete de herramientas lingüísticas y de extracción textual, en fase beta[7], para que toda persona pueda explorar, analizar y obtener una mejor información de textos y documentos escritos en español, gallego, inglés y portugués (Gamallo, 2016).

Linguakit ofrece un conjugador verbal, un resumidor, un corrector, un traductor, un identificador de idioma, un analizador de frecuencias de palabras, un analizador de sentimiento, palabras clave en contexto, un reconocedor de entidades, un extractor de palabras clave, un extractor multipalabra y un etiquetador morfosintáctico.

Por su interés para nuestra investigación, analizamos con Linguakit el contenido del editorial que publicó WikiLeaks el 1 de septiembre de 2011, en el que justifica su decisión de publicar en bruto la totalidad de los cables diplomáticos de Estados Unidos. También sometemos al mismo análisis el comunicado que publicaron un día después los medios colaboradores de WikiLeaks en el *Cablegate*. En concreto, analizamos el contenido del artículo publicado el 2 de septiembre de 2011 en el periódico británico *The Guardian*, principal actor en esta alianza de medios y en la pugna dialéctica con Julian Assange en la crisis del *Cablegate*. En ambos casos, el

[7] La fase beta de un software es la etapa en la que se presenta la primera versión completa del programa informático, pero con posibles fallos que serán subsanados en un proceso de aprendizaje y de notificaciones de errores mediante pruebas de usuario, en las que se pueden proponer soluciones de fallas y otras mejoras. Es la fase intermedia en el ciclo de desarrollo de un software, entre la fase alfa y la versión estable. Por lo tanto, los resultados obtenidos con un software beta pueden mostrar algún error y ser diferentes a los conseguidos con otra versión mejorada o con otro software con las mismas aplicaciones. En la cultura hacker del software libre los programas están en permanente fase beta, sujetos a variaciones y mejoras constantes y abiertas.

análisis se hace sobre el cuerpo de los artículos, excluyendo los titulares. Los resultados obtenidos del análisis de ambos textos son comparados para establecer diferencias y similitudes en los discursos de los medios tradicionales y del nuevo medio, WikiLeaks. Para ello, nos valemos de funcionalidades para el análisis lingüístico y la analítica textual.

De las herramientas incluidas en la categoría de Análisis Lingüístico de Linguakit usamos el analizador de frecuencias, cuyas características principales son:

- Proporciona información del número de caracteres (con y sin espacios en blanco), palabras y frases, además de la cantidad de lemas diferentes.
- Evalúa la variedad léxica del texto, calculada como una ratio del número de lemas entre el número de palabras.
- Calcula además la frecuencia de las palabras contenidas en un texto atendiendo a su categoría gramatical.

Del módulo de Analítica Textual utilizamos el analizador de sentimiento, el extractor de palabras clave, el extractor multipalabra y el reconocedor de entidades.

- Analizador de sentimiento (o de opinión): cuando incluimos un texto en el analizador de sentimiento, el sistema le asigna un valor entre -1 y 1 a cada frase, midiendo así su grado de positividad o negatividad, o bien le asigna un valor igual a 0, si se trata de una frase neutral. El resultado se calcula en porcentaje de positividad o negatividad. El sistema es, por lo tanto, un clasificador que se basa en un modelo construido sobre dos recursos léxicos: por un lado, el sistema emplea léxicos polarizados, es decir, un vocabulario ya clasificado como positivo, negativo o neutro y, por otra parte, utiliza el corpus de entrenamiento, que consiste en el aprendizaje del sistema mediante información recopilada de otras colecciones de enunciados. Además, el analizador de sentimiento de Linguakit incorpora información gramatical, esto es, tiene en cuenta la inclusión de adverbios negativos que pueden cambiar la polaridad de una palabra con la que están ligados sintácticamente.

- Extractor de palabras clave: extrae las unidades léxicas más importantes de un texto y las clasifica según su grado de relevancia. Este extractor se basa en un modelo de frecuencias observadas y frecuencias estimadas. En una primera fase, se identifican todos los candidatos a ser términos básicos (palabras simples monoléxicas) mediante un etiquetador morfosintáctico, seleccionándose como candidatos todas las unidade léxicas etiquetadas como nombres (comunes y propios), adjetivos y verbos. En una segunda fase, los términos se ordenan por relevancia, que se calcula mediante el *termhood*, es decir, el grado en que una unidad lingüística está relacionada con conceptos específicos del dominio, o dicho de otra forma, la probabilidad de que un término forme parte del dominio Así, el sistema mide la relevancia de un término básico (*termhood*) calculando el peso de los vocablos en el texto mediante los test estadísticos con los que realiza una comparación entre la frecuencia observada de las palabras del texto con la frecuencia estimada, es decir, con la frecuencia que deberían tener esas palabras en el corpus ideal o corpus de referencia (datos esperados), que abarca varios géneros y dominios: periodístico, técnico, literario, redes sociales, etc., con un tamaño de 100M.
- Extractor multipalabra: integra dos procesos en los que, en primer lugar, se identifican los candidatos a términos multipalabra, o expresiones pluriléxicas, que deben pertenecer a un patrón gramatical (nombre-preposición-nombre, adjetivo-nombre, nombre-adjetivo, etc.), excluyéndose artículos y determinantes, y en segundo lugar, se ordenan de mayor a menor relevancia siguiendo medidas de asociación estadísticas. En este caso, la relevancia se define por el concepto *unithood*, que se refiere al grado de fuerza y cohesión entre las unidades léxicas que constituyen los sintagmas y colocaciones, aplicándose solamente a unidades pluriléxicas. Una *nube* de los términos multipalabra más relevantes nos ayuda a identificar los temas clave sobre los que gira el texo.

  Estas dos herramientas lingüísticas resultan muy útiles para la detección de un tema de una forma rápida y automática, lo que facilita enormemente la clasificación documental y el etiquetado.

- Reconocedor de entidades: esta herramienta permite extraer de manera automática de un texto los nombres de persona, de lugar, de organización, cantidades, fechas, etc. Es decir, introduciendo un texto podemos saber automáticamente de quién habla, dónde se sitúa lo narrado, qué organizaciones se mencionan, cuándo tuvieron lugar los acontecimientos descritos en el texto o las cifras a las que se hace referencia. El funcionamiento del Reconocedor de Entidades está basado en un modelo en el que se combinan algoritmos de aprendizaje automático con un análisis morfosintáctico; así, según el tipo de palabra, el contexto o la posición gramatical, el algoritmo del sistema es capaz de encontrar las entidades que aparecen en un texto y puede clasificarlas según se trate de personas, organizaciones, lugares, fechas y cantidades.

5.2.5. Monitorización, métricas y analítica web

La recogida y análisis de datos de la presencia, actividad, impacto e influencia de WikiLeaks en Internet y su comparación con los momentos de máximo impacto en los medios de comunicación de masas es el principal pilar sobre el que se sostiene la investigación empírica en nuestro caso de estudio para dilucidar la efectividad de la estrategia informativa de WikiLeaks, es decir, cuándo, cómo y por qué esta organización fue más popular y su mensaje caló más en la opinión pública.

La análitica web surgió a principios de la década de 1990, casi al mismo tiempo que las páginas web comerciales fueron ocupando Internet. Según el programa de formación Actívate de Google, en su Curso de Analítica Web Online, ésta se puede definir como "la recolección, medición, análisis y reporte de los datos que se extraen de la navegación de los usuarios por un sitio web para poder comprender y optimizar su uso" (Google)[8]. El objetivo final es convertir en conocimiento los datos y la información extraídos.

Los medios digitales nos permiten la medición inmediata, en tiempo real, y la recolección de datos históricos. En Internet podemos medirlo prácticamente todo con

[8] Esta definición está tomada del Curso de Analítica Web que el autor de esta tesis hizo en la plataforma *online* Actívate de Google, en mayo de 2014. Se puede encontrar más información sobre esta plataforma de aprendizaje en la siguiente dirección: https://www.google.es/landing/activate/home/ (último acceso: 20 de septiembre de 2015).

unos márgenes de error muy bajos y una inversión económica relativamente baja, o incluso gratuita.

5.2.5.1. Dilemas éticos y ventajas

El desarrollo de las ciencias sociales computacionales, los avances en la teoría y modelización de redes complejas, la disponibilidad de datos masivos en los medios sociales en línea y la sofisticación de técnicas y herramientas para recopilarlos y analizarlos han generado oportunidades sin precedentes para explorar los fenómenos humanos y sociales en una escala global, para identificar patrones de conducta individuales y grupales, y para diseñar modelos predictivos del comportamiento de los sistemas tecnosociales (Lazer *et al.*, 2009; Vespignani, 2009).

Las herramientas de monitorización y analítica web se han convertido en instrumentos fundamentales para los investigadores que quieren seguir temas de actualidad, medir el impacto e influencia de un mensaje, de un acontecimiento o de una campaña en Internet, estudiar comportamientos sociales en línea y analizar el impacto de cualquier organización, institución, empresa, marca, partido político, líder de opinión o cualquier individuo cuya existencia haya sido volcada en la Red.

Monitorizar y analizar el tráfico de una página web, o las conversaciones y comportamientos en las redes sociales en línea, se ha convertido en una práctica común con la masificación de la llamada web social y el desarrollo y auge de software diseñado para auscultar las redes de comunicación electrónicas. Particularmente, las redes sociales *online* están conformando una nueva esfera pública que modifica y reestructura los mecanismos para el debate y las interacciones sociales, articulando un nuevo modelo de participación abierta y aparentemente horizontal, cercano al modelo de democracia deliberativa que se opone al tradicional sistema de democracia representativa. Redes sociales, blogs, foros en línea y medios de masas *socializados* han convertido Internet en un vasto depósito de comentarios sobre cualquier tema imaginable, una enorme fuente de información para la investigación en Ciencias Sociales (Thelwall, Wouters y Fry, 2008). De hecho, la disponibilidad de datos sociales a gran escala accesibles en Internet está transformando radicalmente la investigación social (Savage y Burrows, 2007).

La web social está siendo explotada principalmente con fines comerciales y políticos, pero también académicos, para obtener datos precisos sobre cómo se forman los estados de opinión, cuáles predominan, quiénes son los actores que más contribuyen a generar un estado de opinión en la Red y cómo esta nueva opinión pública se materializa en comportamientos grupales y procesos sociales. El uso de aplicaciones para la monitorización de las redes de comunicación, la recogida sistemática de datos y su análisis permite trazar de una manera discreta los procesos por los que se configura la opinión pública en la Red sobre una amplia gama de temas, en muchos casos sin interacción con los sujetos investigados, sin su consentimiento, sin que sepan que están siendo objeto de estudio, lo cual ha suscitado dilemas éticos y críticas sobre la investigación en Internet, referidos principalmente a los derechos de los individuos cuando son comprometidos (Bassett y O'Riordan, 2002; Enyon, Schroeder, y Fry, 2009; Hookway, 2008; White, 2002; Boyd y Crawford, 2012).

Sin embargo, estos dilemas se suavizan cuando el análisis de comportamientos sociales no necesita ni compromete a individuos identificables; entonces, el dilema principal pasa a ser la manera en que los datos se tratan y analizan, el fin para el que se utilizan y quiénes los gestionan. Uno de los temores principales es a que la ciencia social computacional pueda ser de dominio exclusivo de empresas privadas y agencias gubernamentales, y de grupos privilegiados de investigadores académicos cuyo trabajo no podría ser refutado o validado por otros investigadores (Lazer *et al.*, 2009). De ahí la necesidad de aplicar principios de la ética hacker en este campo que conduzcan al desarollo de software ético libre y de código abierto que garantice derechos y libertades de los sujetos humanos de investigación y el acceso público a los datos recopilados y a los resultados de su análisis.

5.2.5.2. Antecedentes

La literatura y los trabajos de investigación sobre técnicas de análisis web son ya muy amplios y encontramos antecedentes sobre los que fundamentar parte de nuestro trabajo metodológico. Por ejemplo, 'Trends in Social Media: Persistence and Decay' (Asur, Huberman, Szabo y Wang, 2011) es un trabajo que demuestra cómo el estudio intensivo de *trending topics* en Twitter proporciona al investigador una base teórica sólida sobre la formación, persistencia y decadencia de un tema en las

redes sociales en línea. 'The Pulse of News in Social Media: Forecasting Popularity' (Bandari, Asur y Huberman, 2012) es una investigación también centrada en Twitter que, a partir de datos y contenidos recogidos de esta red social, establece un modelo predictivo sobre la propagación de contenidos en las redes y su potencial influencia en la opinión pública. En 'Quantifying the Invisible Audience in Social Networks' (Bernstein, Bakshy, Burke y Karrer, 2013) se combinan datos de encuestas y de registros a gran escala en Facebook para comparar la percepción que los usuarios de esta red tienen sobre su comunidad y el tamaño real del público al que alcanzan sus mensajes. 'Structural Diversity in Social Contagion' (Ugander, Backstrom, Marlow y Kleinberg, 2012) aborda los procesos de contagio en Facebook, principalmente en fenómenos sociales como las modas, las opiniones políticas, la adopción de nuevas tecnologías y decisiones financieras. 'Geography of Twitter Networks' (Takhteyeva, Gruzdb y Wellmanc, 2012) identifica, a partir de la recolección de grandes datos, cómo las distancias geográficas, el territorio físico y el idioma influyen en los vínculos sociales que se configuran en esta red.

Un estudio previo del que incluimos sus resultados en esta tesis es 'Who Says What to Whom on Twitter' (Wu, Hofman, Mason y Watts, 2011), donde se analiza la producción, el flujo y el consumo de la información en esta red social para establecer patrones de comportamiento e identificar a aquellos sujetos con mayor poder para viralizar la información. Por otro lado, 'Competition Among Memes in a World with Limited Attention' (Weng, Flammini, Vespignani y Menczer, 2012) analiza 120 millones de *retweets* en un periodo de cuatro meses, generados por 12,5 millones de usuarios distintos que utilizaron 1,3 millones de *hashtags*, con el objetivo de conocer los procesos por los que determinados temas reciben más atención que otros en un entorno de saturación informativa.

La monitorización *online* y el análisis de datos web han sido también aplicados en la investigación sobre los movimientos de protesta y desobediencia civil. 'The Geospatial Characteristics of a Social Movement Communication Network' (Conover, Davis, Ferrara, McKelvey, Menczer y Flammini, 2013) resuelve —a partir del análisis de 600.000 *tweets* en un periodo de treinta y seis semanas que cubre el nacimiento y la maduración del movimiento anticapitalista estadounidense *Occupy Wall Street*— cómo los objetivos y necesidades de un movimiento de protesta se reflejan en los

patrones geográficos de su red de comunicación, y cómo estos patrones difieren de los de la comunicación política tradicional.

En esta misma línea, 'The Digital Evolution of Occupy Wall Street' (Conover, Ferrara, Menczer y Flammini, 2013) examina el desarrollo en un tiempo de quince meses de la actividad comunicacional en Twitter sobre el movimiento *Occupy Wall Street* para analizar sus cambios, la evolución del compromiso de sus participantes, sus intereses y su conectividad. 'The Arab Spring| The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolution' (Lotan, Graeff, Ananny, Gaffney, Pearce y Boyd, 2011) detalla cómo se produjo y diseminó la información en Twitter durante las revoluciones en Túnez y en Egipto en el año 2011. El libro *Tecnopolítica: la potencia de las multitudes conectadas. El sistema red 15M, un nuevo paradigma de la política distribuida* (Torent, 2013) es otro trabajo que combina distintos métodos experimentales de análisis de redes y datos para explicar, a partir del caso del movimiento de los *indignados* en España, la importancia de la relación entre multiplicación de las prácticas tecnopolíticas a través de redes sociales humanas y digitales, de organización, acción y comunicación colectiva, la toma del espacio urbano y la explosión emocional de indignación y empoderamiento, que dan lugar a un sistema red autónomo y autoorganizado, una multitud conectada capaz de comportamientos colectivos inteligentes.

Por último, 'The Dynamics of Protest Recruitment through an Online Network' (González-Bailón, Borge-Holthoefer, Rivero y Moreno, 2011) estudia los patrones de reclutamiento en Twitter para la protesta social, tomando como caso de estudio las movilizaciones masivas que tuvieron lugar en España en mayo de 2011.

5.2.5.3. Acceso restringido *vs* acceso libre: *growth hacking* adaptado al ámbito académico

La importancia que la comunicación pública ha adquirido en los nuevos espacios globales de interacción social ha hecho que proliferen nuevos métodos y herramientas que permiten medir y analizar con gran precisión la actividad en esta nueva esfera pública ciberespacial, con múltiples variables. El enorme flujo de información y el ingente volumen de datos que se generan continuamente en redes sociales *online* y páginas web, a partir de las acciones de cientos de millones de

usuarios, pueden ser monitorizados y analizados con los instrumentos apropiados. Hoy, existe una gran variedad de herramientas en línea y de software descargable para medir en Internet comportamientos y procesos sociales. Algunas de esas herramientas son gratuitas, pero generalmente limitan las variables, el volumen y el espacio temporal para la recogida de datos, lo que *a priori* es un hándicap para el investigador que quiere realizar un análisis amplio, profundo y preciso, sin limitaciones.

El auge de la investigación pública y privada en la Red ha hecho que los desarrolladores de herramientas de analítica web hayan creado potentes servicios de pago y software privativo para procesar ingentes cantidades de datos y medir prácticamente sin límites toda la actividad que se genera en páginas web o redes sociales. Estas aplicaciones permiten hacer seguimientos en tiempo real y obtener también datos históricos masivos de múltiples usuarios y conversaciones para el análisis cuantitativo y cualitativo. Sin embargo, estas herramientas suelen ser muy costosas y no son accesibles a cualquiera, pues se suelen diseñar para su uso en empresas y laboratorios privados, o para grupos de investigación con grandes recursos económicos. Para nosotros hubiese sido de gran utilidad aplicar estos instrumentos en el trabajo empírico; sin embargo, estaban muy por encima de nuestras posibilidades y se descartaron por su alto coste. Pese a ello, consideramos importante detallar primero cuáles fueron las principales herramientas que se seleccionaron como prioritarias para la monitorización, recogida de datos y análisis del fenómeno WikiLeaks, para luego explicar cuáles fueron las seleccionadas finalmente para estas tareas.

Lo que pretendemos con esto es mostrar las ventajas que nos podrían proporcionar en futuras investigaciones herramientas más sofisticadas para el análisis de datos masivos, pero también queremos demostrar que, pese a las limitaciones que debemos enfrentar cuando usamos herramientas de análisis gratuitas, su uso adecuado y combinado permite, mediante técnicas de triangulación, paliar algunas deficiencias y conseguir datos precisos y sustanciales que garantizan la validez y rigurosidad de la aproximación al objeto de estudio. En el uso de herramientas gratuitas también subyace una intención de ser coherentes con el hilo argumental de esta tesis. Por último, pretendemos demostrar cuán importante es para la investigación académica el desarrollo de software libre del que se beneficie toda la comunidad científica.

Aunque no podemos incluir los programas utilizados en esta investigación en

la categoría de software libre[9] —dado que su código fuente no está liberado y no pueden ser copiados ni modificados—, en éstos subyacen tibiamente valores de la ética hacker, ya que proporcionan acceso libre —aunque con algunas limitaciones, generalmente temporales y de volumen— a datos e información que pueden ser utilizados por cualquier individuo conectado a la Red. De hecho, en el campo del márketing *online* se conoce como *growth hacking* al uso combinado y creativo de diversas herramientas y técnicas innovadoras de bajo coste o gratuitas para hacer crecer un producto, un servicio, una marca, etc.

Analítica, creatividad y curiosidad se abrazan en el *growth hacking*, que bebe, como es obvio, de la cultura hacker. Así que cuando diseñamos nuestra metodología, pensamos que sería interesante adaptar esta tendencia mercadotécnica al campo de la investigación científica y consideramos que era oportuno hacerlo en nuestro caso.

5.2.5.4. Herramientas de pago

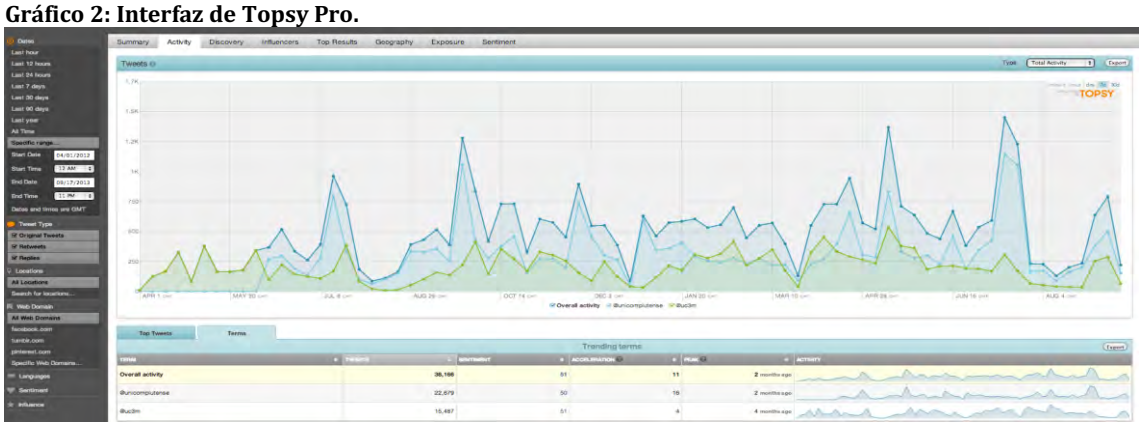
A continuación vamos a resumir las características principales de las herramientas de pago que preseleccionamos como útiles en la fase de diseño de la metodología, para nuestra monitorización y análisis en redes sociales, concretamente, en Facebook y Twitter, las más populares y masivas, y paradigmas de la nueva esfera pública digital. La idea era combinar al menos dos de estas tres herramientas para cotejar los datos extraídos y asegurar resultados y análisis más fiables, siendo Topsy[10] la herramienta que evaluamos como la más idónea para el análisis en Twitter y Sysomos, la más completa para un análisis más global en Internet, por su enorme base de datos de distintos medios sociales. Se incluyó también Pirendo por ser una propuesta española puntera en inteligencia y analítica en redes sociales

[9] La Free Software Foundation lo define así: "«Software libre» es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre». En inglés a veces decimos «libre software», en lugar de «free software», para mostrar que no queremos decir que es gratuito". Disponible en: http://www.gnu.org/philosophy/free-sw.es.html (último acceso: 18 de octubre de 2015).

[10] Durante la fase de revisión y corrección de esta tesis, Apple cerró Topsy, dos años después de haberlo comprado por 200 millones de dólares. Topsy era una herramienta estadística que gozaba de gran prestigio entre expertos en analítica en Twitter. Pese a ello, Apple decidió eliminarlo en diciembre de 2015. Sin embargo, consideramos necesario mantener esta referencia, primero, porque fue parte de nuestra primera selección de herramientas; en segundo lugar, porque nos seguía sirviendo como ejemplo de servicio de pago de calidad para la analítica en redes sociales, y en tercer lugar, poque su desaparición —y la de otros servicios en línea— nos motivaba aún más a defender el uso de software libre.

Topsy Pro Analytics

Gráfico 2: Interfaz de Topsy Pro.



Fuente: Topsy.

Topsy fue una de las herramientas en línea más populares para el análisis de datos en Twitter. Permitia recopilar datos en tiempo real e históricos. Con Topsy se obtenía acceso a un índice de todos los *tweets* y contenido web referenciado desde el año 2006. Su tecnología garantizaba que cada mención de cualquier término o cuenta se registrase con precisión, contabilizando el total de publicaciones sobre un tema o usuario. El análisis se podía refinar por geografía, sentimiento, idioma, influencia y/o fechas. Así, se podía comparar la exposición de un conjunto de términos, etiquetas o usuarios, pudiendo conocer su número total de impresiones potenciales y su evolución en el tiempo. También se podían ver los *tweets*, enlaces, fotos o vídeos sobre cualquier tema en cualquier período de tiempo, ordenados por relevancia.

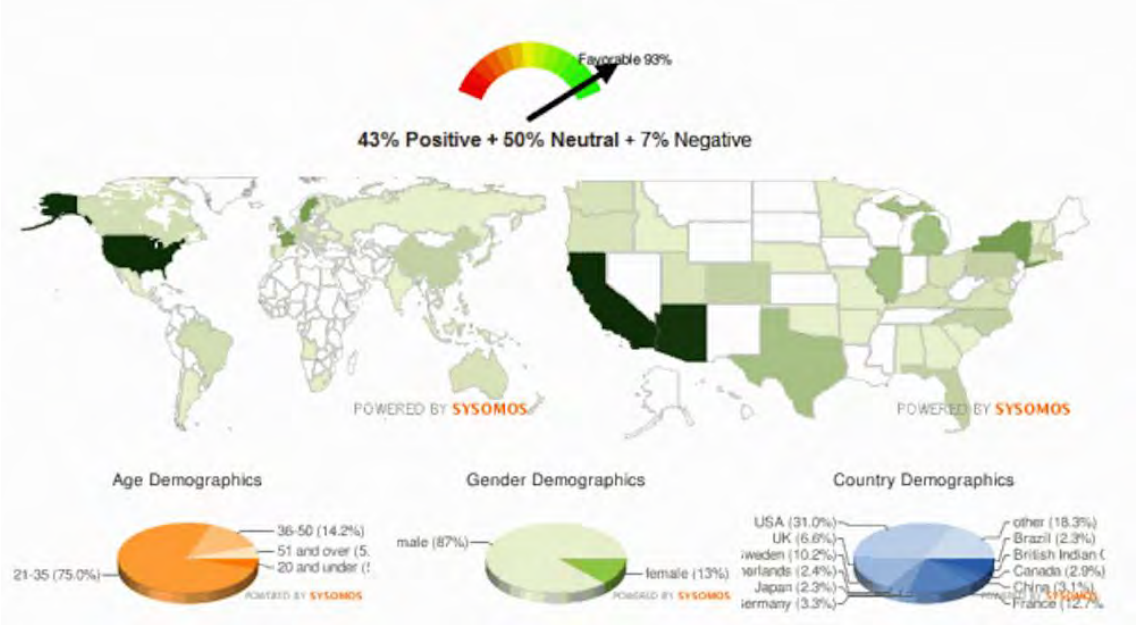
Con Topsy se podía analizar el impacto geográfico de un usuario o tema en Twitter, pudiendo filtrar datos por países, regiones y ciudades de todo el mundo. La herramienta proporcionaba información sobre la ubicación de más del 90 por ciento de los *tweets* publicados, lo que permitía al investigador centrar su análisis en lugares específicos y detectar diferencias geográficas. Esta herramienta permitía también identificar a los líderes de opinión en Twitter, a los usuarios más influyentes en cualquier tema y las publicaciones más relevantes en un momento determinado. Además, medía el grado de sentimiento (positivo/negativo) que genera un tema o un usuario de Twitter y las conversaciones generadas en torno a cualquier página web, independientemente de la forma en que se acortase y se compartiese su URL.

Topsy mostraba también las principales palabras clave relacionadas con un tema y detectaba al instante las publicaciones más relevantes.

Con Topsy se podía comparar datos para diferentes rangos de fechas, lugares, términos, *hashtags* o temas. Por último, esta herramienta permitía exportar al disco duro del ordenador los contenidos y los análisis obtenidos, para que el investigador pudiese guardarlos y disponer de éstos en cualquier momento.

Sysomos

Gráfico 3: Ejemplo de visualización de datos de Sysomos.



Fuente: Sysomos.

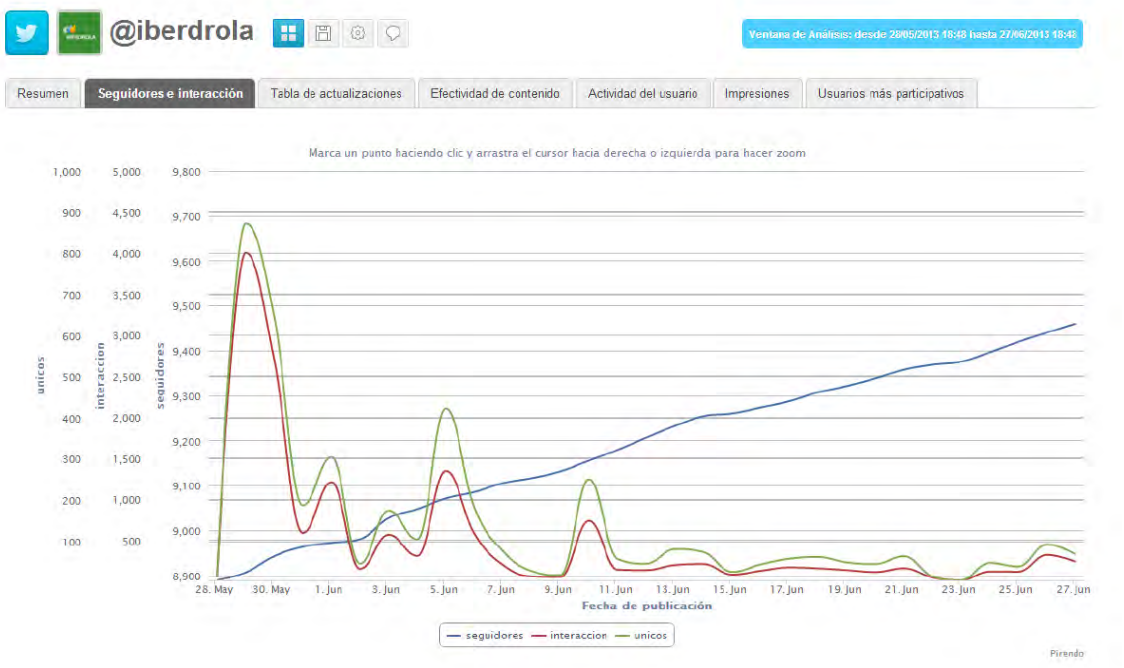
Sysomos es fruto de un proyecto de investigación nacido en la Universidad de Toronto y está considerada una de las mejores herramientas de monitorización y análisis de medios en línea. Para los investigadores ofrece la solución MAP, para el estudio en profundidad, análisis histórico y preparación de informes. El servicio MAP ofrece consultas ilimitadas y acceso a una enorme base de datos con miles de millones de conversaciones en medios sociales que datan de años. Esa base de datos se actualiza constantemente con la actividad que se va generando en blogs indexados, redes sociales, *wikis*, foros *online*, fuentes de noticias, etc.

La herramienta también aporta datos sobre el volumen de actividad que genera un tema, dónde se origina, quién está hablando sobre ello y la autoridad de los implicados en la conversción. Sysomos permite identificar a usuarios que lideran conversaciones y la formación de estados de opinión. El investigador puede también medir y comparar el alcance, la participación y el impacto de una marca, usuario o

tema frente a otros. También facilita datos geográficos y demográficos detallados, con información sobre participantes en medios sociales, sus conversaciones, localización, edad, sexo, idioma, profesión, etc. Además, se puede medir el sentimiento que genera un tema o usuario en tres grados: positivo, negativo o neutro.

Pirendo

Gráfico 4: Ejemplo de gráfico de Pirendo



Fuente: Pirendo.

Herramienta de origen español para monitorizar y medir Twitter, Facebook y YouTube. Por defecto, la herramienta ofrece datos del último año en el que se inicia la monitorización, aunque los administradores de Pirendo ofrecen como servicio adicional recoger el historial de la actividad de las cuentas analizadas. A través de paneles de seguimiento de cuentas, palabras clave o etiquetas se pueden conocer estadísticas constantemente actualizadas sobre conversaciones ocurridas en Twitter y Facebook, y se obtienen gráficos sobre su evolución. También se puede diseñar informes a medida de datos segmentados por localizaciones, idiomas, redes, comunidad de seguidores, etc.

Con esta herramienta se puede obtener datos de Twitter sobre la cantidad de usuarios que han publicado *tweets* con un *hashtag* o palabra clave y la cantidad de

impresiones logradas. También se puede medir la cantidad de *tweets* que se han enviado con una etiqueta o palabra clave y la cantidad de *retweets* que incluyen el término. Pirendo también mide la amplificación, es decir, la relación de *retweets* conseguidos y respuestas recibidas respecto al total de la conversación. Otros datos que se pueden extraer de Twitter son: número de seguidores de una cuenta, cantidad de impresiones logradas por un usuario, número de menciones a un usuario, número de respuestas recibidas, número de *retweets* logrados por un usuario, cantidad de *tweets* del usuario que han sido marcados como favoritos, aplauso (la relación de favoritos logrados respecto a los mensajes enviados).

Respecto a Facebook, Pirendo mide el número de fans de una página, número de fans activos que interactúan o participan en las publicaciones de la página, porcentaje de fans activos, actualizaciones de una página, número de "me gusta" logrado por las publicaciones de la página en un rango de tiempo analizado, cantidad de comentarios en la página, cantidad de veces que se han compartido publicaciones de la página en un periodo concreto, puntuación Pirendo de la página (se obtiene otorgando tres puntos a cada acción ejecutada mediante el botón "compartir", dos puntos a cada comentario y un punto a cada "me gusta"), el aplauso (la relación entre el número de "me gusta" conseguidos y las publicaciones del administrador de la página), amplificación (relación entre las veces que se comparte contenido respecto al total de publicaciones del administrador) y conversación (relación de comentarios recibidos por publicación). Pirendo también permite medir palabras clave en Facebook, aportando datos del número de usuarios que han publicado incluyendo la palabra analizada, la cantidad de publicaciones, el valor de las interacciones, el número de "me gusta" recibidos y la cantidad de comentarios realizados por los usuarios en dichas publicaciones.

5.2.5.5. Analítica web: triangulación de datos aplicada

Identificar los momentos de máximo impacto de WikiLeaks en Internet nos permite identificar sus hitos históricos, nos ayuda a construir el relato sobre este fenómeno y nos permite establecer relaciones causales.

Para medir el grado de dependencia de WikiLeaks a los medios tradicionales de masas necesitábamos primero hacer una monitorización de la presencia, actividad,

impacto e influencia que la organización ha tenido en Internet, en general, y en las dos principales redes sociales en las que WikiLeaks está activa, en particular: Twitter y Facebook. Para ello hemos recurrido a un conjunto de herramientas *online* gratuitas y *freemium* de analítica web y de monitorización para tal fin: Google Insights For Search, Google Trends, Alexa, Trendistic, Wildfire App, TweetStats y PeopleBrowsr.

El análisis se completa con los datos públicos que ofrece Wikipedia como termómetro del interés que genera un tema en Internet. Los datos recogidos abarcan un periodo de tiempo comprendido entre finales del año 2006, cuando nació WikiLeaks, hasta la primavera de 2012, cuando se inició la publicación de más de cinco millones de correos electrónicos de la agencia de inteligencia global Stratfor. De esta manera, podemos comparar el impacto que las sucesivas filtraciones de WikiLeaks tuvieron en el tiempo, principalmente entre las publicaciones en el año 2010 del vídeo *Collateral Murder*, los documentos secretos de las guerras en Irak y Afganistán, y el *Cablegate* —que marcaron un cambio en la estrategia de difusión de WikiLeaks—, y las filtraciones de Stratfor, el primer gran golpe de efecto de WikiLeaks tras romper relaciones con los periódicos con los que había colaborado en el año 2010.

Las herramientas seleccionadas nos permiten obtener información sobre la actividad, tráfico, impacto e influencia de WikiLeaks en la Red, y con ellas podemos comprobar si el papel de colaboradores de los medios tradicionales de masas influyó, y cómo, en el impacto que obtuvo WikiLeaks en el ciberespacio, en qué grado esos medios tradicionales contribuyeron a popularizar WikiLeaks y a expandir su mensaje, y si existe aún una preponderancia de los medios de información tradicionales de masas sobre los llamados medios alternativos y sobre nuevos modelos de organización informativa como WikiLeaks en la era de Internet y de la sociedad red. Para ello, nos valemos de los datos que ofrecen los gráficos que hemos generado con las herramientas utilizadas para esta investigación, que describen en una línea de tiempo el comportamiento de los usuarios en las búsquedas en Google con el término *wikileaks*, datos sobre tráfico de la página web de la organización, datos sobre actividad en la página de WikiLeaks en Wikipedia, y datos sobre su popularidad, impacto e influencia en las dos redes sociales más importantes: Twitter y Facebook.

Los datos arrojados en estos gráficos en una línea de tiempo nos permiten identificar los periodos de mayor impacto, influencia y actividad de WikiLeaks en

Internet, y con ellos podemos verificar si coinciden o no con los momentos claves en los que algunos medios tradicionales de masas influyentes colaboraron con WikiLeaks, evaluar su incidencia y comparar el impacto mediático y social de las distintas filtraciones.

Como ya hemos explicado, una opción hubiese sido utilizar un par de herramientas sofisticadas de pago de empresas de analítica web que ofrecen completísimos datos y gráficos sin restricciones en volumen de datos y tiempo, pero por su alto coste se optó por usar un conjunto de herramientas *online* gratuitas y *freemium* cuyos resultados, comparados y cruzados, ofrecen datos suficientes y pruebas palmarias para llegar a conclusiones válidas.

También existía la opción de proponer el desarrollo de un software *ex profeso* para esta investigación, el cual hubiese sido, por supuesto, un software libre para su uso, modificación y mejora por parte de cualquiera. Pero esta tarea requería la labor de un experto programador dedicado en exclusiva a un proyecto que hubiese sido, por sí solo, otra tesis.

A continuación se explican las funcionalidades de cada una de las herramientas seleccionadas y su aplicación en esta investigación.

Google Insights For Search

Herramienta de estadísticas de búsqueda de Google que permite comparar patrones de volumen de búsqueda en determinadas regiones, categorías, intervalos de tiempo y propiedades[11]. Se introdujo el término *wikileaks* y se aplicaron los siguientes filtros para la búsqueda:

- Búsqueda en la Web.
- Ámbito geográfico: todo el mundo
- Periodo: diciembre 2006 - abril 2012.
- Todas las categorías.

[11] Este servicio fue clausurado por Google el 27 de septiembre de 2012 —poco después de nuestra primera recogida de datos— y se fusionó con Google Trends.

Google Trends

Con esta herramienta calculamos el número de consultas de la palabra *wikileaks* en relación con el total de búsquedas realizadas en Google en un periodo de tiempo determinado, y el volumen de noticias publicadas relacionadas con el término de búsqueda introducido en Google Trends[12]. Aplicamos los siguientes filtros:

- Ámbito geográfico: todas las regiones.
- Periodo: 2004 - 2012 (esta herramienta no permite personalizar la búsqueda entre dos fechas, pero sí admite resultados aislados de los últimos 30 días y 12 meses, además de anuales y mensuales desde el año 2004, y por defecto ofrece los resultados del máximo periodo que analiza Google Trends, desde el año 2004 hasta el presente).

Alexa

Mide la reputación de un sitio web con el número de *sites* que tienen enlaces apuntando a esa página y provee información acerca del tráfico del sitio web para clasificarlo entre todas las páginas del mundo. Alexa recoge información de los usuarios que tienen instalada en su navegador la aplicación Alexa Toolbar, a partir de la cual se generan estadísticas del tráfico de la página y del comportamiento de los usarios en el sitio. Esto hace que las estadísticas generadas estén muy sesgadas en la mayoría de casos, aunque para páginas web con grandes volúmenes de tráfico —las que figuran entre las cien mil primeras del ránking Alexa, incluida la de WikiLeaks— su fiabilidad es bastante alta y reconocida, reportando datos aproximados que permiten evaluar con ciertas garantías el impacto de un sitio web. Este servicio permite obtener resultados acumulados durante los últimos siete días, último mes, últimos tres y seis meses o un tiempo máximo de dos años, que ha sido el periodo elegido para nuestra investigación. Se utilizaron los siguientes índices de medición para la página web oficial de WikiLeaks (http://wikileaks.org/):

- Ránking de tráfico: indica el puesto de un *site* entre todos los del mundo a partir del número de usuarios que lo visitan y de las páginas vistas. El gráfico recoge datos de los 100.000 sitios más transitados.

[12] Este servicio se utilizó antes y después de que fuese integrado con Google Insights For Search.

- Alcance: porcentaje estimado de usuarios totales de Internet que han visitado diariamente el sitio web.
- Páginas vistas: porcentaje estimado de páginas del sitio web vistas por los usuarios cada día. Aquellas mismas páginas que son vistas múltiples veces por un mismo usuario durante el mismo día sólo se toman en cuenta una vez. Hablamos, pues, de promedio de páginas únicas vistas al día del global del tráfico que analiza Alexa en Internet.

Trendistic

Herramienta similar a Google Trends para analizar tendencias y medir el impacto que ha tenido un tema en Twitter[13]. Se obtuvo un gráfico con datos del impacto del término *wikileaks* entre diciembre de 2006 y diciembre de 2011.

Wildfire App

Sistema de monitorización que ofrece datos por día y datos acumulados de la evolución del número de seguidores en Facebook y Twitter[14]. Se analizaron las cuentas de WikiLeaks en estas dos redes sociales: <https://www.facebook.com/wikileaks> y <https://twitter.com/wikileaks>.

TweetStats

Esta herramienta ofrece un gráfico del volumen de *tweets* publicados cada mes por un usuario de Twitter, desde el inicio de su actividad en esta red social. Recogimos los datos de la cuenta de WikiLeaks desde enero de 2009 hasta mayo de 2012.

PeopleBrowsr

Herramienta *freemium*[15] que permite en su versión gratuita obtener información sobre el impacto e influencia de un tema, tendencia o palabra clave en Twitter, contabilizando el número de menciones diarias en una línea de tiempo de mil

[13] Este servicio fue clausurado también en el año 2012, después de nuestra recogida de datos.
[14] La plataforma Wildfire App fue comprada en el año 2012 por Google, que en 2014 inició un proceso gradual de desactivación del servicio.
[15] *Freemium* es un modelo de negocio que combina servicios básicos gratuitos y otros avanzados de pago.

días máximo. Se introdujo el término *wikileaks* en una búsqueda que nos devolvió datos desde octubre de 2009.

Wikipedia

También recogimos datos estadísticos de la página de WikiLeaks en Wikipedia. Entendemos que esta enciclopedia libre en línea, como una de las principales fuentes secundarias de información en Internet y termómetro del interés que puede suscitar un tema, nos permite obtener resultados válidos para esta investigación. Según datos de Alexa de octubre de 2015, Wikipedia es el séptimo sitio web más popular del mundo.

Cuadro 3: Sitios web más populares según Alexa.

1	Google.com
2	Facebook.com
3	Youtube.com
4	Baidu.com
5	Yahoo.com
6	Amazon.com
7	Wikipedia.org
8	Qq.com
9	Twitter.com
10	Google.co.in

Fuente: elaboración propia a partir de los datos recogidos en octubre de 2015 de http://www.alexa.com/topsites.

En esta tesis aportamos datos sobre el interés generado por WikiLeaks entre los editores de Wikipedia, la evolución de la edición de su *wiki*, así como datos sobre el tráfico a la página de WikiLeaks en Wikipedia.

La principal crítica a Wikipedia, especialmente expresada por la rama científica y enciclopedista más ortodoxa, cuestiona el rigor de sus artículos, pero también la calidad de éstos, y apunta a la existencia de sesgos, lo cual resta fiabilidad a la Wikipedia, en opinión de sus críticos. Sin embargo, en diciembre de 2005 la revista *Nature* llevó a cabo un estudio en el que se comparó la precisión de una muestra de artículos de Wikipedia con otra de la Enciclopedia Británica. Los expertos evaluaron

cuarenta y dos artículos sobre temas científicos, incluyendo biografías. Los artículos fueron comparados por colaboradores académicos que permanecieron en el anonimato, siguiendo la práctica común para las revisiones de artículos de revistas científicas. La investigación de *Nature* reveló que los artículos de Wikipedia mostraban de media cuatro errores u omisiones, mientras que en la Enciclopedia Británica la media fue de tres. El estudio concluyó que Wikipedia se acerca a la Enciclopedia Británica en términos de precisión de sus páginas de ciencia (Giles, 2005).

Aunque Wikipedia cuenta con un sistema de reglas y procesos de control para intentar garantizar la más alta calidad y rigor, los *wikipedistas* admiten ser conscientes de la existencia de basura literaria entre sus millones de páginas y, por ello, buscan cubrirse las espaldas con un documento de "Limitación general de responsabilidad" que advierte a los usuarios de que "la información que encuentren en esta enciclopedia no necesariamente ha sido revisada por expertos profesionales que conozcan los temas de las diferentes materias que abarca, de la forma necesaria para proporcionar una información completa, precisa y fiable"[16]. El documento pretende evitar cualquier responsabilidad legal derivada de la aparición de información inexacta, errónea o difamatoria, o del uso que cualquier usuario pueda hacer de la información contenida en sus páginas o que esté enlazada desde o hacia ellas. En todo caso, los *wikipedistas* presumen de que "la mayoría de las veces" el usuario encontrará en su sitio web "información exacta y valiosa".

Dicho esto, debemos subrayar que no es nuestra intención llevar esta tesis al debate científico sobre la fiabilidad de Wikipedia, pues nuestro interés no radica en el contenido, en la calidad, veracidad u objetividad de los artículos de Wikipedia, sino en la actividad que éstos generan, tanto la relativa a las ediciones como a las consultas de usuarios de Internet. Lo que pretendemos con los datos de edición y tráfico de la página de WikiLeaks en Wikipedia es comparar estos resultados con los demás datos obtenidos en nuestra investigación para poder evaluar el interés que genera el fenómeno Wikileaks en la Red y determinar si los periodos de máxima actividad en el *wiki* de esta organización coinciden con los momentos de máximo impacto mediático y/o máxima actividad en las redes sociales y búsquedas en Google.

[16] Disponible en: https://es.wikipedia.org/wiki/Wikipedia:Limitación_general_de_responsabilidad (último acceso: 7 de octubre de 2015).

5.2.5. Análisis de las portadas de *The New York Times*, *The Guardian*, *Le Monde* y *El País*

Para complementar la recogida de datos en Internet analizamos las portadas de las ediciones en papel de los medios que colaboraron con WikiLeaks en el *Cablegate*, en el periodo comprendido entre el 29 de noviembre de 2010, cuando se inició la publicación de las filtraciones de cables diplomáticos de Estados Unidos, y el 31 de diciembre de 2010. Delimitamos este análisis *a posteriori*, con los resultados del impacto de las filtraciones de documentos secretos en Internet, que nos permitieron acotar el intervalo de tiempo en el que se produjo el apogeo de WikiLeaks.

Primero, constatamos que las portadas de las ediciones en papel de los periódicos aún conservan un gran significado y poder simbólicos, tanto para los medios como para el público. Esto lo podemos comprobar en Twitter, donde los medios tradicionales avanzan ahora sus portadas en papel como argumento de venta, con miles de usuarios ejerciendo de prescriptores de éstas con sus *retweets*.

Ilustración 1: *The New York Times* [nytimes]. (2015, Jun 27). The front page of *The New York Times* for Saturday, June 27. http://t.co/FuLRxMEoBs [Tweet]. Recuperado de: https://twitter.com/nytimes/status/614757609233645568.

El análisis de contenido de las portadas en papel nos pareció sustancial por cuanto nos servía para completar el estudio de correlaciones entre el impacto de las filtraciones de WikiLeaks en los medios tradicionales y el impacto social y político de estas revelaciones viralizadas en la Red. Entendimos que esto nos ayudaría además a comprender el papel que todavía juegan los medios de masas en la configuración de la agenda pública y su influencia sociopolítica en la era de la sociedad red.

Por todo esto, pensamos que sería de gran utilidad cuantificar el espacio que los medios colaboradores de WikiLeaks en el *Cablegate* dedicaron expresamente a las filtraciones de documentos en sus portadas, pero también a otras informaciones relacionadas con éstas y el universo WikiLeaks. Para ello utilizamos PageOneX, un software libre de código abierto bajo licenza GNU, accesible en Internet y premiado por la American Political Science Association. Ideada por el arquitecto español Pablo Rey-Mazón (2013), esta herramienta está diseñada para la codificación, análisis y visualización de informaciones en las portadas en papel de periódicos de todo el mundo, que siguen siendo el termómetro para medir la *temperatura* de un tema, esto es, la importancia que estos medios de masas otorgan a las noticias publicadas.

La versión alfa de PageOneX fue desarrollada en el año 2012 por Rey-Mazón, junto con Ahmd Refat, en el marco del programa anual Google Summer of Code, en el Berkman Center for Internet & Society de Harvard. Ya en abril de 2013 se lanzó la versión beta, esta vez en el Center for Civic Media del MIT Media Lab, fruto de la colaboración de Rey-Mazón con el hacker e ingeniero informático Edward L. Platt y el investigador y tecnólogo Rahul Bhargava.

Lo que hicimos con PageOneX fue codificar las noticias relacionadas con WikiLeaks en dos categorías: 1) noticias sobre los cables diplomáticos y 2) noticias sobre otros acontecimientos relacionados con WikiLeaks. Una vez hecha la codificacion, obtenemos en la línea de tiempo seleccionada la evolución del porcentaje de superficie que ocupan los contenidos de cada categoría, lo que nos permite observar el progreso del caso WikiLeaks en cada medio y comparar los resultados obtenidos con los datos históricos recogidos del impacto de WikiLeaks en la Red, para intentar establecer o descartar relaciones causales.

5.2.6. Fuentes secundarias

Como complemento a los datos recogidos en nuestra investigación recogemos los resultados obtenidos en la encuesta internacional que Ipsos realizó en marzo de 2011 sobre las filtraciones de WikiLeaks y la figura de Assange. También recogemos los resultados del estudio 'Getting Personal: Personification vs. Data-Journalism as an International Trend in Reporting about Wikileaks', dirigido por la profesora Andrea Czepek, de la Jade University of Applied Sciences de Wilhelmshaven (Alemania), en el cual analizaron 1.125 noticias sobre WikiLeaks publicadas en diciembre de 2010 en medios de comunicación de España, Francia, Alemania, Suecia y Reino Unido.

El instituto global de investigación de mercados Ipsos realizó entre el 2 y 14 de marzo de 2011 una encuesta internacional a una población de 18.829 ciudadanos, entre 18 y 64 años, de 24 países: Argentina, Australia, Bélgica, Brasil, Canadá, China, Francia, Gran Bretaña, Alemania, Hungría, India, Indonesia, Italia, Japón, México, Polonia, Rusia, Arabia Saudita, Sudáfrica, Corea del Sur, España, Suecia, Turquía y Estados Unidos. El objetivo de este estudio, titulado *Ipsos Global @ dvisory: Julian Assange and WikiLeaks*, era concluir de qué manera las actividades de WikiLeaks, su página web y la figura de Julian Assange impactaron en la opinión pública mundial, en todos los continentes, tras las grandes filtraciones del año 2010. En cada país, la población encuestada fue de alrededor de mil individuos, excepto en Argentina, Bélgica, Indonesia, México, Polonia, Arabia Saudita, Sudáfrica, Corea del Sur, Suecia y Turquía, con muestras de quinientos individuos en cada uno de estos países, aproximadamente. Esto se hizo para equilibrar la demografía y garantizar que la composición de la muestra se ajustaba al censo de población adulta de cada país.

La profesora Andrea Czepek es la responsable de la investigación 'Getting Personal: Personification vs. Data-Journalism as an International Trend in Reporting about Wikileaks', cuyos resultados fueron presentados en el XXVI Congreso Internacional de Comunicación (CICOM), celebrado en la Universidad de Navarra los días 4 y 5 de julio de 2011. Los investigadores hicieron un análisis comparativo de contenidos de medios de comunicación de cinco países europeos: España, Alemania, Francia, Suecia y Reino Unido. En total, analizaron 1.125 noticias de prensa y televisión en las que se mencionaba a WikiLeaks, fechadas entre el 1 y el 31 de diciembre de 2010, coincidiendo con el apogeo del *Cablegate*. Para ello, seleccionaron

dos periódicos por país[17] y los espacios informativos de sus televisiones públicas. Además de criterios formales, incluyeron variables como el género periodístico, actores participantes, el tema, el principal país sobre el que se informaba, el marco de la información, el sesgo, el contenido, los valores expresados, el nivel de investigación y las fuentes utilizadas. La siguiente tabla muestra los medios seleccionados por cada país, su relación con WikiLeaks y el número de piezas analizadas.

Tabla 1: Medios analizados en la investigación 'Getting Personal: Personification *vs.* Data-Journalism as an International Trend in Reporting about Wikileaks'.

Country	Media type	Media included in the sample	Official cooperation with Wikileaks	Number of items "Wikileaks" December 2010
France	public tv	TF 1	no	5
France	newspaper	Le Monde	yes	55
France	newspaper	La Libération	partially (host website)	65
Germany	public tv	Tagesschau (ARD)	no	32
Germany	newspaper	Westdeutsche Allgemeine (WAZ)	no	30
Germany	newspaper	Frankfurter Allgemeine (FAZ)	no	45
Germany	news magazine	Der Spiegel	yes	17
Spain	public tv	La 1 (TVE)	no	22
Spain	newspaper	El País	yes	56
Spain	newspaper	ABC	no	25
Sweden	public tv	SVT	no	46
Sweden	newspaper	Dagens Nyheter	no	146
Sweden	newspaper	Svenska Dagbladet	no	148
UK	public tv	BBC	no	67
UK	newspaper	The Guardian	yes	266
UK	newspaper	The Times	no	100
Total				1125

Fuente: Diversity of journalisms. Proceedings of the ECREA Journalism Studies Section and 26th International. Conference of Communication (CICOM) at University of Navarra, pp. 98-99.

[17] Entre los medios seleccionadas se incluyeron las cuatro publicaciones europeos que colaboraron en el *Cablegate*: *The Guardian*, *Le Monde*, *El País* y *Der Spiegel*. En el caso de Alemania, debido a que *Der Spiegel* es una revista semanal, se sumaron los diarios: *Frankfurter Allgemeine* y *Westdeutsche Allgemeine*.

5.2.7. Participación activa en las filtraciones de Stratfor

Nuestra investigación es ampliada utilizando el método de observación participante. De acuerdo con las propuestas de Becker y Geer (1958), el objetivo principal de este modelo de investigación debe ser la descripción de distintos hechos, situaciones y acciones que suceden en un escenario social concreto. Para Wolf ([1987], 1996), se trata del método más adecuado para estudiar la sociología de los emisores en el proceso informativo.

El 4 de agosto de 2012, WikiLeaks nos ofreció la posibilidad de unirnos a su grupo de investigación internacional dedicado a los conocidos como *Global Intelligence Files* (*GI Files*), un inmenso archivo de 5.543.061 correos electrónicos filtrados de la empresa de inteligencia global Stratfor —"una especie de CIA corporativa" (Assange 2014: 21) con sede en Texas—, datados entre julio de 2004 y diciembre de 2011. La invitación confidencial que recibimos de WikiLeaks nos permitió introducirnos dentro del flujo comunicativo y, valiéndonos del método de observación participante, recoger y obtener información y datos fundamentales sobre las rutinas productivas operantes en éste.

Esta invitación de WikiLeaks tuvo un doble valor para nosotros:

1) Pudimos conocer de primera mano, desde dentro, los métodos y procesos colaborativos de WikiLeaks y su estrategia para tratar la información y difundirla con el máximo impacto posible, lo cual nos permitió aplicar la línea de investigación observacional conocida como *newsmaking* —centrada en las rutinas productivas de los emisores— en un ecosistema de trabajo novedoso, virtual, propiciado por una organización red, donde cada nodo es independiente y goza de plena autonomía en el proceso de exploración, selección, producción, publicación y difusión de la información, aunque WikiLeaks impone ciertas condiciones para participar en este proceso colaborativo que veremos más adelante.

2) Nos dio la oportunidad de desarrollar la propia labor de investigación, edición y publicación periodística aplicada en complejos procesos de gestión y difusión de enormes volúmenes de información confidencial y secreta, enfrentándonos además a profundos dilemas éticos que necesitábamos experimentar en primera persona para comprender mejor la lucha dialéctica entre privacidad y secreto.

La fase de observación estuvo ligada a nuestra hipótesis de que el impacto de WikiLeaks depende de la atención que le presten los grandes medios de información convencionales y de que las filtraciones sean controladas con las labores clásicas del periodismo, y no simplemente liberadas en bruto en un sitio web. La observación, en este caso, es sobre el medio, sobre los instrumentos y procedimientos con los que se opera en éste y sobre los flujos de comunicación e información. Dado que la nuestra es una observación participante mediada por la virtualidad, en un entorno en el que no existe interacción humana, en el que las comunicaciones son electrónicas y automatizadas, donde todo se produce en una pantalla y nuestra experiencia es unipersonal, subyace una autoobservación del propio sujeto investigador, que es a la vez sujeto investigado por sí mismo, que registra los procedimientos de su participación y los resultados de su propia actividad. Pero también hay introspección y autoevaluación de nuestra propia experiencia para generar un conocimiento autorreflexivo crítico adquirido por autoobservación.

Todo el proceso de registro y acceso a la base de datos de WikiLeaks, uso de herramientas, búsqueda de información, producción periodística, publicación y difusión es explicado en los resultados de nuestra investigación.

No hay barrera, cerradura ni cerrojo que puedas imponer a la libertad de mi mente.

—Virginia Woolf.

I. HACKERS

I.1. ¿QUÉ ES SER HACKER?

Seis décadas después de que este vocablo inglés se reinventase como neologismo para definir y configurar una actividad, para algunos, una actitud, para otros, primigeniamente vinculada al mundo de la computación, aún hoy ni lexicógrafos ni periodistas ni científicos, ni siquiera la propia comunidad hacker, han logrado un pacto para dilucidar qué es ser hacker. Recorriendo las elásticas interpretaciones aportadas sobre el *hacking*, encontramos desde auténticas loas y apologías al hacker como héroe de la revolución computacional (léase el venerado libro *Hackers: Heroes of the Computer Revolution*, de Steven Levy, escandalosamente inédito en español tres décadas después de su publicación, en 1984), hasta diatribas y escarnios públicos dedicados a una comunidad tradicional y sistemáticamente mancillada, particularmente por los medios de comunicación de masas, que han generalizado y globalizado el término *hacker* como sinónimo de delincuente informático y potencial terrorista. La propia comunidad hacker, que ha pasado ya por varios estadios evolutivos en las últimas seis décadas —vinculados al desarrollo de la computación, de las redes de comunicación electrónicas y de tecnologías digitales de la información y la comunicación—, tampoco ha ayudado mucho a acotar y a consensuar una definición sobre el *hacking* y sobre quiénes lo ejercitan.

La polisemia de la palabra *hack* y de sus derivados tira de ésta en direcciones opuestas, hacia un binarismo axiológico. Sus diferentes significados se han formado y definido por un sistema de antinomias u oposiciones binarias que han contrbuido a organizar una comprensión y evaluación social del *hacking* reducida al ámbito de la computación, restringiendo la valoración de este fenómeno social complejo a un totalistarismo moral. Sin embargo, el *hacking* no puede ser reducido a la simple

dualidad maniquea del bien y del mal, ni tampoco debe ser constreñido a la actividad computacional, pues ha evolucionado a un ideal humano que abarca cualquier actividad creativa que conlleve una actitud vital motivada por la curiosidad de explorar los límites de lo técnico y lo humano, y por desafíos y retos personales para la solución de problemas no resueltos. Así, a nadie debe extrañar que se hable de hackers matemáticos, hackers artistas o hackers periodistas.

> Cualquier explorador decente tiene que tener un poco de espíritu hacker o acabará haciendo lo que hace todo el mundo y no descubrirrá nada nuevo. Un buen periodista siempre debe dudar de lo que se le dice y pensar en maneras de evitar limitaciones para encontrar una historia decente. El espíritu hacker es una parte del espíritu humano y siempre lo ha sido (Goldstein, 2009: 314)[18].

Sin embargo, aún hoy el *hacking* se identifica exclusivamente como actividad computacional ilícita que se presta al sensacionalismo mediático, al cual han contribuido también algunos grupos hackers:

> Los niveles habituales de bombo publicitario de los medios que existen en torno a cualquier historia noticiable se han agravado en el caso del *hacking* y del hacktivismo por el hecho de que estas actividades se relacionan, a los ojos de la opinión pública, con la zona recóndita de la computación. El proceso se exacerba aún más con el anonimato y la naturaleza no física de estos actos mediados por ordenador. La combinación de estos factores hace un brebaje embriagador para aquéllos que quieren sensacionalismo sobre el tema, y elementos de los inicios de la comunidad del *hacking* aportaron su propio tipo de retórica a esta mezcla con la adopción de nombres de grupos llamativamente inquitantes tales como The Legion of Doom, Bad Ass Mother Fuckers y Toxic Shock.
>
> Los sentimientos sociales preexistentes de vulnerabilidad tecnológica pueden ser deliberadamente exagerados por aquéllos que tienen diversos grados de mentalidad hacker, pero tal bombo publicitario sólo refleja los temores más arraigados sobre el cambio tecnológico en general (Jordan y Taylor, 2004: 22)[19].

La estigmatización social de los hackers surge principalmente de las representaciones valorativas y dramatizadas de los medios de comunicación de masas (Hollinger y Lanza-Kaduce, 1988: 119; Kane, 1989). Meyer y Thomas (1990) estiman que la definición de los hackers que han proporcionado los medios de comunicación, y la falta de una comprensión clara de lo que significa verdaderamente ser hacker, han dado como resultado una errónea aplicación de la etiqueta *hacker* a todas las formas

[18] Todas las citas del libro *The Best of 2600: A Hacker Odyssey* (2009), editado por Emmanuel Goldstein, fueron traducidas del texto original, en inglés, por el autor de esta tesis.
[19] Todas las citas del libro de Jordan y Taylor *Hacktivism and Cyberwars: Rebels with a cause?* (2004) fueron traducidas del texto original, en inglés, por el autor de esta tesis.

maliciosas de computación. Esta identificación del delincuente informático con los hackers se considera "despreciativa y un insulto a la amplia comunidad hacker, que está trabajando para hacer del mundo un lugar mejor para todos" (Goldstein, 2009: 504-505).

En plena campaña antihacker, en la transición de la década de 1980 a 1990, autores como Meyer y Thomas desafiaron la explicación maniquea difundida por los medios de comunicación de masas de que "los hackers pueden ser entendidos simplemente como profanadores de un orden económico y moral sagrado" (Meyer y Thomas, 1990: 5)[20]. De los datos obtenidos por estos autores en los Bulletin Board Systems hackers se puede colegir que "en contra de su imagen mediática, los hackers evitan la destrucción deliberada de datos o causar daño alguno al sistema" y "su objetivo principal es la adquisición de conocimientos" (1990: 15). En esta línea argumentativa, Bruce Sterling, atendiendo a los criterios de Levy, describe el *hacking* como "la determinación por hacer el acceso a las computadoras y a la información tan libres y abiertos como sea posible", lo cual se traduce en "la convicción más sincera de que la belleza puede ser hallada en las computadoras" y en la certeza de que "la elegante estética de un programa perfecto puede liberar la mente y el espíritu" del individuo (Sterling, 1992).

I.1.1. Definiciones

Para llegar a una redención conceptual del hacker y de su actividad tenemos que recurrir a las múltiples e intrincadas definiciones que se le han dado históricamente a esta palabra. La primera e ineludible referencia a la que acudimos es la definición que se recoge en el Jargon File, el diccionario por antonomasia de la cultura hacker. El propio glosario, revisado y actualizado sucesivamente desde su creación, en 1975, aclara que la acepción original de la palabra *hacker* se refería "a alguien que hace muebles con un hacha". Aislado este significado, el Jargon File aplica hasta ocho acepciones diferentes para intentar deslindar el nuevo uso de la palabra *hacker* como neologismo surgido en la era digital:

[20] Todas las citas de las obras de Meyer y Thomas (1990, 1992) son traducciones propias de los textos originales, en inglés. Las citas de su artículo 'The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground' (1990) incluyen los números de página del documento original, publicado en su versión elecrónica por la Electronic Frontier Foundation, también incluido por F. Schmalleger en el volumen *Computers in Criminal Justice* (1990), publicado por Wyndham Hall Press.

> 1. Una persona que disfruta explorando los detalles de los sistemas programables y cómo estirar sus capacidades, a diferencia de la mayoría de los usuarios, que prefieren aprender sólo lo mínimo necesario. RFC1392, el Glosario de los Usuarios de Internet, útilmente amplifica esto como: una persona que se deleita en tener un profundo conocimiento del funcionamiento interno de un sistema, ordenadores y redes informáticas en particular.
>
> 2. Quien programa con entusiasmo (incluso obsesivamente) o disfruta de la programación en lugar de teorizar acerca de la programación.
>
> 3. Una persona capaz de apreciar el valor del hackeo.
>
> 4. Una persona que es buena programando rápidamente.
>
> 5. Un experto en un programa informático en particular, o una persona que con frecuencia trabaja usando cierto programa. Por ejemplo, «un hacker de Unix programador en C»[21].
>
> 6. Un experto o un entusiasta de cualquier tipo. Uno puede ser un hacker de la astronomía, por ejemplo.
>
> 7. Aquel que disfruta el reto intelectual de superar o eludir creativamente limitaciones.
>
> 8. [Obsoleta] Un intruso malicioso que trata de descubrir información sensible entrometiéndose en algún sistema. Por lo tanto, hackers de contraseñas, hackers de acceso a redes. El término correcto para este sentido es cracker.
>
> (The on-line hacker Jargon File, version 4.4.7, 29 de diciembre de 2003)[22].

Para completar estas ocho acepciones, el Jargon File dilucida que el término *hacker* también tiende a connotar la pertenencia a la comunidad global definida por la Red. También implica que la persona así descrita es percibida como alguien que suscribe alguna versión de la ética hacker[23]. Y se concluye:

> Es mejor ser descrito como un hacker por otros que describirse a uno mismo de esa manera. Los hackers se consideran una especie de elite (una meritocracia basada en la habilidad), aunque suelen recibir amablemente a nuevos miembros. Existe, pues, una cierta satisfacción del ego en identificarse a uno mismo como un hacker (pero si dices ser uno y no lo eres, rápidamente te etiquetarán como falso). (The on-line hacker Jargon File, version 4.4.7, 29 de diciembre de 2003).

Definiciones simplistas y consensuadas por los lexicógrafos las encontramos en los diccionarios académicos, en los de las empresas editoriales y en los diccionarios gratuitos en línea que se han popularizado entre los usuarios de Internet. En lengua inglesa, el Oxford Dictionary registra las siguientes acepciones para la palabra *hacker*:

---

[21] Las definiciones 1, 2, 3, 4 y 5 están correlacionadas, según el Jargon File.
[22] Todas las citas del Jargon File son traducciones propias de su versión 4.4.7, en inglés.
[23] Véase el apartado I.3 dedicado a la ética hacker, página 113.

1. Una persona que usa una computadora para obtener acceso no autorizado a datos.

   1.1 Un entusiasta y hábil programador o usuario de computadoras.

2. Una persona o cosa que machetea o corta bruscamente.

El popular diccionario en línea Wordreference, por su parte, incluye varias definciones para el término *hacker* en inglés, recogidas de distintas fuentes lexicográficas.

A. Random House Learner's Dictionary of American English:

   1. Una persona o cosa que corta.
   2. Una persona no cualificada en un deporte.
   3. Una persona que es excelente en la programación de computadoras [jerga].
   4. Un usuario de computadoras que obtiene de manera ilegal acceso a sistemas informáticos restringidos [jerga].

B. Collins Concise Dictionary Inglés © HarperCollins Publishers

   1. Una persona que corta.
   2. [Jerga] Un fanático de las computadoras, especialmente alguien que desde un ordenador personal asalta el sistema informático de una empresa, gobierno, etc.

A pesar de su extendido y común uso en español, la Real Academia Española (RAE), inexplicablemente, no se había atrevido a incluir la palabra *hacker* en el Diccionario de la lengua española hasta su vigesima tercera edición, presentada el 17 de octubre de 2014. La definición oficial en castellano es tan escueta como reveladora del desconocimiento de los académicos sobre el tema:

> hacker: pirata informático.

El diccionario de la lengua española Espasa-Calpe, en su edición de 2005, incluye una acepción con una connotación también delictiva para la palabra *hacker*, aunque es más explicativa que la de la Real Academia Española[24]:

[24] Véase en el diccionario en línea Wordreference: http://www.wordreference.com/definicion/hacker (último acceso: 20 de octubre de 2013).

> hacker
> (voz i.) com. INFORM. Persona muy aficionada y hábil en informática que entra ilegalmente en sistemas y redes ajenas.

La enciclopedia libre, políglota y colaborativa más grande del mundo, la Wikipedia, ofrece en su edición española una descripción más detallada y próxima a la realidad hacker:

> El término hacker tiene diferentes significados. Según el diccionario de los hackers, es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien. De acuerdo a Eric S. Raymond, el motivo principal que tienen estas personas para crear software en su tiempo libre, y después distribuirlos de manera gratuita, es el de ser reconocidos por sus iguales. El término hacker nace en la segunda mitad del siglo XX y su origen está ligado con los clubes y laboratorios del MIT (Wikipedia).

La Wikipedia se explaya en distintos significados atribuidos al término *hacker*:

> En informática, un hacker es una persona que pertenece a una de estas comunidades o subculturas distintas, pero no completamente independientes:
>
> - En seguridad informática este término concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".
> - Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT. Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. «How To Become A Hacker». El [[Request for comments|RFC]] 13926 amplía este significado como "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas".
> - La comunidad de aficionados a la informática doméstica, centrada en el hardware posterior a los setenta y en el software (juegos de computadora, crackeo de software, la demoscene) de entre los ochenta/noventa.
> - Se utiliza la palabra Hacker para describir a una persona que practica la programación informática, con una especie de pasión artística, o que forma parte de la cultura de los hackers, es decir al grupo de programadores que históricamente están en los orígenes de Internet, en Linux y en la World Wide Web.

- Desde que se usó por primera vez la palabra Hacker ésta ha sido mal utilizada, mal interpretada y encasillada en un contexto errado, antes que nada, aclaremos que el término Hacker no tiene nada que ver con actividades delictivas, si bien muchos Hackers cometen errores, la definición no tiene nada que ver con ello.
    - Definición 1: Término para designar a alguien con talento, conocimiento, inteligencia e ingenio, especialmente relacionadas con las operaciones de computadora, redes, seguridad, etc.
    - Definición 2: Persona que disfruta aprendiendo detalles de los sistemas de programación y cómo extender sus capacidades, tan intensamente como, al contrario, muchos usuarios prefieren aprender sólo el mínimo necesario.

Lejos de las acepciones consensuadas por las jerarquías del Estado-nación e inoculadas en la sociedad a través de los diccionarios y de los medios de comunicación de masas, "en los círculos hackers, el hack es más ampliamente definido como un intento de usar la tecnología de un modo original, poco ortodoxo e inventivo" (Jordan y Taylor, 2004: 6). En esta línea argumental, Turkle ([1984] 2005) ofrece una conceptualización de los elementos principales del *hacking* confirmados posteriormente por el estudio de Taylor (1999), y que, elevado a la categoría de "Santo Grial", existe independientemente de las computadoras. Para Turkle, el atributo esencial de un *hack* reside en el pragmatismo ecléctico con que los hackers abordan de forma característica cualquier tecnología. Pero el abordaje debe ser apasionado.

La pasión es la pulsión hacker. Jérémie Zimmerman —*cypherpunk*[25] cofundador de la organización La Quadrature du Net para la defensa del derecho al anonimato en la Red— define al hacker como "un apasionado de la tecnología, alguien a quien le gusta entender cómo funciona la tecnología no para quedar atrapado en ella, sino para mejorar su funcionamiento" (Assange *et al*., 2012: 67).

Al hablar de tecnología no sólo nos debemos referir a tecnología informática, sino a cualquier conjunto de conocimientos, instrumentos y procedimientos técnicos que, aplicados de forma lógica, permiten al ser humano modificar su entorno material o virtual para satisfacer sus necesidades, esto es, un proceso combinado de pensamiento y acción con la finalidad de crear soluciones útiles.

[25] Este neologismo se ha traducido en español como *criptopunk*. Nosotros decidimos usar en esta tesis la forma original inglesa.

El *hacking* —como vanguardia del postindustrialismo informacional anticipado conceptualmente por Alain Touraine (1969) y Daniel Bell (1973), y su prognosis, reexaminada y precisada lúcidamente por Manuel Castells (1997, 2001, 2006, 2009)— nació ligado a la computación y a los laboratorios tecnológicos de las universidades estadounidenses en la década de 1960. Es por ello que tradicionalmente se ha identificado casi exclusivamente como una actividad informática. En aquellos centros, jóvenes entusiastas de la computación crearon una comunidad, una nueva cultura que traza su historia desde los primeros sistemas de tiempo compartido[26] y los más tempranos experimentos en ARPAnet (Advanced Research Projects Agency Network), el embrión de Internet. Sin embargo, el *hacking* se ha asociado dentro de la propia comunidad hacker a otras actividades no vinculadas directamente con la computación, especialmente con el *lock-picking*[27], la primigenia expresión del *hack* (Levy, 1984), cuyo "placer está en «vencer» a la cerradura. Rompen, entran y luego se van. No están tras los bienes materiales, sino tras la emoción del triunfo" (Turkle, [1984] 2005: 213). Este interés en introducirse en lo hermético está, desde los orígenes de la cultura hacker, intrínsecamente ligado al ideal de la libertad de información.

> El hacker de los años sesenta [del siglo XX] no fue más allá de la apreciación de las habilidades del *lock-picking*, tanto en lo relativo a los bloqueos físicos que prohíben el acceso a las salas de ordenadores, como a los sistemas de protección de software, tales como contraseñas y esquemas de encriptación; también creía en que la información nace para ser libre, incluidos el código fuente escrito por el propio hacker y su conocimiento sobre el funcionamiento interno de distintos sistemas (Hannemyr, 1999)[28].

En 1987, Theodore T. Tool publicó lo que pronto sería considerada la *Biblia* del ganzuado, el *MIT Guide to Lock Picking*, revisado cuatro años después por su propio autor y considerado un texto de culto no sólo entre los hackers por sus afinidades con su cultura, sino también entre cerrajeros. La teoría del *lock-picking* habla de explotar los defectos mecánicos, de usar trucos para abrir cerraduras y candados con características o defectos particulares, causando menos daños que con la fuerza bruta. En definitiva, se trata de un *hack* y, como tal, es admirado por los hackers

[26] Conocido más popularmente como *time-sharing*, se trata de un método de acceso a un ordenador por parte de varios usuarios a la vez. El tiempo compartido ejecuta programas separados de forma concurrente, intercambiando porciones de tiempo asignadas a cada programa (usuario). Fue introducido en computación en la década de los años sesenta del siglo XX.
[27] Arte de liberar o abrir cerraduras, candados y cualquier sistema de cierre sin la llave o mecanismo original para hacerlo y sin causar o minimizando daños. Está considerado una suerte de *hacking* físico.
[28] Todas las citas de Hannemyr fueron traducidas del texto original, en inglés, por el autor de esta tesis.

informáticos por su manifiesta analogía con el arte de abrir *cerraduras* y *candados* de sistemas computacionales. Cualquier sistema cerrado, opaco, es un desafío para los hackers. Cualquier sistema hermético esconde misterios que deben ser resueltos y secretos que deben ser revelados[29].

Esto se ha aplicado principalmente en la computación, pero la cultura hacker ni se limita a esta ciencia ni está restringida por una tecnología; se puede encontrar en casi cualquier actividad humana creativa, de manera que "la cantidad de cosas *hackeables* ahí fuera es prácticamente ilimitada" (Goldstein, 2009: 314). No es el medio, sino el fin lo que determina la naturaleza hacker de un individuo y de su actividad. Así lo han reconocido los propios hackers computacionales:

> La mentalidad hacker no se limita a esta cultura de software-hacker. Hay personas que aplican la actitud hacker a otras cosas, como la electrónica o la música —en realidad, la puedes encontrar en los más altos niveles de cualquier ciencia o arte—. Los hackers de software reconocen estos espíritus afines en otros lugares y pueden llamarlos también «hackers», y algunos afirman que la naturaleza hacker es realmente independiente del medio particular en el que trabaja el hacker (Raymond, 2001).

Goldstein es más radical en la conceptualización del hacker:

> Creo que hay un montón de gente ahí fuera que no tiene ningún interés en las computadoras, pero que son verdaderos hackers. Lo cierto es que hay un montón de cosas en el mundo que hackear. Muchas son hardware —digital, electrónico, mecánico— y mucho es puramente conceptual. Lo importante es poder decir que tienes la mente de un hacker. Eso significa pensar siempre con originalidad, cuestionar lo que otros asumen que es verdad, intentar hacer algo de otra manera sólo por ver qué sucede, no escuchar a quienes te dicen que hay que atenerse a las reglas por la simple razón de que ellos son la reglas, e inevitablemente meterse en serios problemas en algún momento (Goldstein, 2009: 313).

Y Stallman proporciona un ejemplo práctico de *hack* aplicado en otras actividades distintas a la computación:

> […] nosotros, los hackers, aún insistimos en que *hack* significa mucho más que aquello de romper la seguridad para el desarrollo informático. Por ejemplo, Lady Gaga es hacker de ropa. Lo que hace con su ropa es emplear su inteligencia con un espíritu juguetón. Y si eres hacker puedes apreciarlo como *hack*. Porque ser hacker no sólo significa que te gusta emplear tu inteligencia con espíritu juguetón, sino también probablemente que gozas viendo que otros lo hacen y cómo lo hacen, que disfrutas viendo sus logros (Richard Stallman, en Quian, 2013c).

[29] Más adelante veremos que para los hacktivistas el propio sistema político y económico también debe ser hackeado, rompiendo los candados que guardan sus secretos y misterios.

Aunque el conocimiento técnico es una ventaja para la actividad hacker, no es esencial para convertirse en hacker. Sin embargo, lo cierto es que lo técnico se presta más y mejor al *hacking* (Goldstein, 2009: 313), no sólo al computacional. Si bien "los hackers han jugado un papel significativo, aunque también controvertido, en la historia de la computación" (Turkle, [1984] 2005: 189), desde sus orígenes han desarrollado y aplicado sus habilidades en una amplia gama de campos mecánicos y tecnológicos, sin restringirse a la computación.

Kane afirma que el *hacking* no es más que modificar una y otra vez las condiciones de un aparato o sistema hasta conseguir de este una respuesta diferente. "En el mundo mecánico de hoy, las oportunidades para este tipo de experimentación son infinitas" (Kane, 1989: 67). Así, existe toda una gama heterogénea de objetos tecnológicos considerados *hackeables*: semáforos, teléfonos, microondas o reproductores de DVD son sólo algunos de los *otros* artefactos con los que los hackers han jugado para desarrollar en ellos usos imprevistos o no supuestos. Utilizar un teléfono para ejecutar funciones que no se presuponían a este aparato es un *hack*; usar habilidades mecánicas para que un automóvil haga cosas que no se suponían también es un *hack*.

Por ejemplo, el primer SMS (Short Messaging Service, o servicio de mensajería corta) fue el resultado de un *hack* de un ingeniero de la empresa Sema Group, Neil Papworth. El primer SMS sen envió el 3 de diciembre de 1992. El objetivo de su emisor fue iniciar un sistema de comunicación rápido y divertido. El primer mensaje que envió decía simplemente "Feliz Navidad" y fue dirigido a su colega en Vodafone, Richard Jarvis. Catorce años después, en plena erupción de la telefonía móvil y con cientos de millones de SMS enviados por todo el mundo, este sistema inspiró otro modo de comunicación que también alteró radicalmente nuestra forma de comunicarnos, de informarnos y de interactuar: Twitter.

La red social del pájaro azul fue fruto de otro *hack*. Su concepto como servicio de comunicación se inspiró en el de los SMS que se envían mediante los teléfonos móviles —con un número de caracteres también limitado, en el caso de Twitter, a 140, y en el del SMS, a 160—, pero en este caso la comunicación es en red, a través de Internet, y sin coste por el uso del servicio. También la invención de los *hashtags* de Twitter —etiquetas de metadatos— fue un *hack*. La idea se le ocurrió al desarrollador

web Chris Messina, quien el 23 de agosto de 2007 publicó un *tweet* en el que propuso usar el símbolo # para agrupar contenido en Twitter y así organizar conversaciones.

Richard Stallman, considerado el gran gurú de la comunidad hacker del software libre, asume que la palabra *hacker* ha tenido diferentes significados desde sus orígenes, aunque hay algo invariable que le permite ofrecer su propia definición:

> Para mí [ser hacker] es gozar del uso de la inteligencia con un espíritu juguetón. Esta definición es mi intento de buscar lo que hay en común entre los varios usos que hemos hecho de este término. La palabra «hacker» se empezó a usar en el MIT y en otras instituciones relacionadas, por ejemplo, en la Universidad de Stanford, ya que había bastante migración de gente entre éstas. Fueron partes de la misma comunidad. El caso es que usábamos la palabra «hacker» de varias formas, pero lo que tenían en común era el uso de la inteligencia con un espíritu juguetón y no necesariamente en la informática. El *hack* era posible también en otras actividades (Richard Stallman, en Quian, 2013c).

Finalmente, Eric S. Raymond (2001) considera que para ser hacker es condición *sine qua non* ser parte de esta cultura, hacer contribuciones a la misma, ser conocido por otros miembros de la comunidad y que éstos te reconozcan como hacker. O como explica Goldstein (2009: 265), "uno no se convierte en hacker diciendo que lo es […]. Ser hacker es un estado de la mente y esto es lo que los medios de comunicación nunca pudieron entender".

Desde la invención del teléfono de Graham Bell y la existencia de los primeros *phone-phreaks* (Goldstein, 2009: xxxvii), hasta el desacato estético y escénico de Lady Gaga, pasando por las computadoras de los gurús del software libre, la cultura hacker es vasta, se extiende en la historia en campos mecánicos, creativos y de pensamiento heterogéneos y sobrepasa los límites conceptuales que el Estado-nación y sus mecanismos institucionales han impuesto a la palabra *hacker* para diseminar e inocular en las masas una idea negativa de ésta.

I.2. ETHOS HACKER

Ya hemos introducido algunas referencias sobre la criminalización de los hackers, en la que los medios de masas han jugado un papel fundamental. La controversia sobre este vocablo se dilucida brevemente en Wikipedia:

> En la actualidad [hacker] se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. Según Helen Nissenbaum[30] que los hackers sean mal vistos ayuda al gobierno y a los poderes privados con dos cosas: 1) a definir lo que es normal en el mundo computacional haciendo creer que un buen ciudadano es todo lo que el hacker no es; 2) a justificar la seguridad, la vigilancia y el castigo (Wikipedia).

Lo cierto es que el *ethos* hacker nada tiene que ver con la idea que ha calado en la opinión pública del *hacking* como acto delictivo. Desde sus propios medios, los hackers han intentado explicar al mundo, con escasa fortuna, su genuino carácter y sus valores. Uno de sus principales *altoparlantes* ha sido el editor de la revista *2600*, Emmanuel Goldstein, con alegatos como el siguiente:

> El *hacking* no es malo. El *hacking* es saludable. Hackear no es lo mismo que robar. El *hacking* descubre defectos de diseño y las deficiencias de seguridad. Por encima de todo, el *hacking* demuestra que el ingenio de una sola mente sigue siendo la herramienta más poderosa de todas. Somos hackers. Siempre lo seremos. Nuestros espíritus no serán aplastados por estos acontecimientos horribles. Llámenos cómplices, compañeros anarquistas, lo que quiera. Tenemos la intención de seguir aprendiendo. Suprimir este deseo es contrario a todo lo que es humano. Al igual que los autores que se levantaron para defender a Salman Rushdie del largo brazo de la histeria, debemos elevarnos para defender a aquéllos en peligro por la caza de brujas contra los hackers. Después de todo, no nos pueden encerrar a todos. Y a menos que lo hagan, el *hacking* está aquí para quedarse (Goldstein, 2009: 206).

Tradicionalmente, la literatura sobre hackers ha tendido a colapsar el *hacking* en un binario moral en el que sus actores son alabados como verdaderos héroes de nuestra sociedad o denunciados y mancillados como villanos (Coleman y Golub, 2008). Sin embargo, Emmanuel Goldstein difiere de esta conceptualización dual:

> Un hacker verdadero irrumpe en computadoras por un desafío. No sale para salvar el mundo o destruirlo. No sale para obtener un beneficio de lo que está haciendo. Por lo tanto, no es justo categorizar al hacker como un criminal al igual que es erróneo decir que es una especie de salvador (Goldstein, 2009: 210).

[30] Helen Nissenbaum scritora y profesora de Medios, Cultura y Comunicación, y de Ciencia Computacional en la New York University y directora del Information Law Institute de dicha universidad.

Como iremos viendo en este trabajo, esta visión dicotómica se perpetúa y se ha agudizado alrededor de la séptima generación de hackers: los hacktivistas. La carga semántica negativa que históricamente ha prevalecido ha condenado socialmente a los hackers no sólo como adictos patológicos a las computadoras y a Internet, gamberros, delincuentes, intrusos, ladrones de información o incluso terroristas cibernéticos (Sandberg, 1994; Slatalla y Quittner, 1995; Shimomura y Markoff, 1996; Schwartau, 2000; Borsook, 2001); también se ha impuesto una mirada vitriólica colectiva a los hackers como individuos asociales, aislados y deshumanizados, subordinados a las máquinas y con comportamientos excéntricos, compulsivos y adictivos que dibujan un perfil análogo al de los drogodependientes[31]. Este argumentario se empezó a viralizar a través de los medios de comunicación de masas a partir de los años ochenta del siglo XX, cuando estos empezaron a poner el foco sobre grupos de expertos en computación que se reunían en los laboratorios de las principales universidades de Estados Unidos, principalmente, pero también en otras zonas del planeta tecnológicamente desarrolladas, con el único afán de escribir nuevo software y desarrollar nuevo hardware de forma colaborativa, desarrollar mejoras y descubrir nuevos usos no previstos en dispositivo tecnológicos. El *hacking* "nunca tuvo nada que ver con ser malicioso o destructivo […], aquella idea errónea fue alimentada por los medios de comunicación de masas" (Goldstein, 2009: xxxvi).

Stallman esclarece cuándo y cómo se empezó a pervertir el significado del *hacking*:

> Lo que sucedió fue que sobre los años 1980-1981 los medios de comunicación se dieron cuenta de nuestra existencia, pero lo hicieron con gran confusión porque sólo se fijaron en un aspecto limitado del *hacking*, en una de las actividades que algunos hackers hacían a veces, la de romper la seguridad informática para ganar acceso a las computadoras. Y para ganar acceso hacía falta usar la inteligencia con un espíritu juguetón. Pero es incorrecto suponer que ser hacker signifique solo romper la seguridad. Lo único que se quería por entonces era poder tener acceso y usar en cualquier momento alguna computadora del MIT para la investigación... No se hizo para dañar nada ni a nadie, sino sólo para romper una regla que bloqueaba el acceso. No lo considerábamos malo, no había por qué hacerlo. Sólo fue algo malo para los autoritarios, para quienes piensan en términos de obediencia. Sin embargo, otros hackers pensaron más allá. En el laboratorio en el que yo trabajaba, el equipo de desarrollo del sistema operativo decidió no introducir seguridad informática. Mucho mejor que romper la seguridad de las computadoras fue no tener seguridad para usar las computadoras sin obstáculos (Richard Stallman, en Quian, 2013c).

[31] En el capítulo dedicado a WikiLeaks veremos cómo el *storytelling* del poder institucional utiliza el mismo viejo argumentario para criminalizar a Julian Assange ante la opinión pública.

Esos chicos *desaliñados* autodenominados hackers estuvieron en el epicentro de la revolución computacional, en el centro de nuestra era tecnológica (Himanen, 2001: vii). Así lo evidencia Seymour Papert —uno de los pioneros de la inteligencia artificial y cofundador del Artificial Intelligence Lab del MIT, junto con Marvin Minsky— cuando coloca a los hackers al frente de las Ciencias de la Computación, como autores de los primeros gráficos por ordenador, de los primeros procesadores de textos, de los primeros videojuegos o de los primeros sistemas de tiempo compartido (Brand, 1987: 56).

Los primeros hackers fueron los artífices de un cambio dramático para el que no aceptaban reglas ni normas, estándares ni dictámines, guías ni convencionalismos. Y no fue una revolución guiada, ni siquiera pactada; no había jerarquías ni control institucional o empresarial, ni siquiera ánimo de lucro ni horarios laborales, ni estética ni apariencia. Aquellos hackers no sólo estaban alterando radicalmente nuestra interacción con el (resto del) mundo, también estaban subvirtiendo tradiciones, convenciones y pactos sociales arraigados y, sobre todo, la ética protestante del trabajo en la que el capitalismo ha asentado sus más sólidos pilares[32].

Stallman niega, sin embargo, que la cultura hacker busque causar revolución alguna.

> Yo no diría que se trate de una revolución. Normalmente los hackers no desean hacer una revolución. Ser hacker no implica ningún deseo de cambiar el mundo. Fundamentalmente es un deseo de lucir tu inteligencia juguetona, como sucede por ejemplo con el poeta cuando compone poemas. En mi artículo 'On Hacking' cito como ejemplo el palíndromo musical *Ma Fin Est Mon Commencement* de Guillaume de Machaut, una pieza del siglo XIV que fue un buen *hack* (Richard Stallman, en Quian, 2013c).

Sin embargo, cualquier *hack*, en cualquier ámbito, supone siempre una novedad, un cambio, una pequeña o gran revolución, poética, tecnológica, periodística, etc. El propio Stallman contradice con su argumento sus propias intenciones de cambiar el sistema de producción y el propio modelo económico del conocimiento mediante el movimiento del software libre, que supone una verdadera revolución dentro del sistema capitalista. El mismo hecho de proponer el flujo libre de información, de promover el acceso abierto al conocimiento y de concebir la tarea

[32] Ir a página 115.

productiva como un juego, un arte, una tarea creativa, libre y compartida, todo ello cuestiona el modelo capitalista de privatización del conocimiento y la automatización y estandarización de la producción. "Para los verdaderos hackers, la diferiencia entre «juego», «trabajo», «ciencia» y «arte» tiende a desaparecer, o a mezclarse en un alto nivel de creatividad" (Raymond, 2001).

Esa miscelánea de radicalismo ético y estético no es comprendida en una sociedad acomodada en sus seguridades contractuales: la seguridad de que vivir en un sistema capitalista abre la puerta a conseguir el sueño dorado de cualquier ciudadano estandarizado, es decir, un contrato de trabajo remunerado, un coche y una casa en propiedad, unas vacaciones y el acceso a bienes y servicios que cubran sus necesidades naturales y artificiales. Todo ello, mediante contrato. Quien no firma ni cumple el *contrato*, está al margen y se convierte en marginal a ojos de los demás. Quien se sale del vallado que delimita el campo de juego social para explorar nuevos espacios es señalado como una amenaza para la seguridad de toda la comunidad, acomodada en el cerco diseñado y protegido por la autoridad.

En el filme *The Village*, de M. Knight Shyamalan (2004), encontramos una inquietante, tenebrosa y clarificadora fábula sobre el mapa de los miedos que la autoridad jerárquica impone al individuo para anular sus inquietudes y garantizar la homogeneización en la que se sustenta el sistema autoritario, por medio de reglas estrictas cuyo incumplimiento debe motivar no sólo una pena de castigo, sino también una condena social y estigmatización del individuo. La radicalidad individual, el espíritu inquieto, juguetón y rebelde, el afán exploratorio e innovador, y la necesidad de compartir nuevos hallazgos con cualquiera dispuesto a escuchar hacen del hacker un individuo *peligroso* para la autoridad (Goldstein, 2009: xxxvi-xxxvii). Sin embargo, la penalización al hacker no parece generar el efecto coercitivo esperado por la autoridad, ya que no reprime la persistencia del hacker en aplicar su curiosidad y la observación en un entorno nuevo y desagradable, el de la prisión física y la sanción social, ni refrena su deseo de compartir sus resultados con otros, pues ese deseo de compartir experiencias es una de las aportaciones hackers más valiosas (Goldstein, 2009: 381).

El hacker no hace más que repetir los procesos que han permitido el progreso social, cognitivo y cultural. Andy Müller-Maguhn —miembro del Chaos Computer

Club, cofundador de la ONG European Digital Rights (EDRI) y director europeo de Internet Corporation for Assigned Names and Numbers (ICANN) entre los años 2000 y 2003— dilucida que "la historia de la raza humana y la historia de la cultura es la historia de copiar pensamientos, modificarlos y procesarlos una y otra vez", por lo que "si tú llamas a eso robar eres un cínico más"; argumento al que se suman Zimmermann, para quien es "consustancial a la cultura que ésta se comparta", y Assange, que señala como problema el proceso de industrialización de la cultura y del conocimiento en Occidente, donde "desde la década de los cincuenta hemos tenido la cultura industrial. Nuestra cultura se ha convertido en un producto industrial" (Assange *et al*., 2012: 80).

El hacker salta las vallas para explorar el bosque y allende, y con sus hallazgos novedosos deslegitima a los sátrapas. La necesidad de ser gobernado y constreñido por una autoridad no existe en la cultura hacker. No en vano, la naturaleza hacker es antiautoritaria (Raymond, 2001). Pero esta actitud no contraviene todo pacto social o norma básica para la convivencia, sino aquella autoridad que limita el ejercicio de la libertad y de la creatividad del individuo por medio del control, la vigilancia, la censura, el secreto, el uso de la fuerza o el engaño.

Un ejemplo práctico de esta mentalidad antiautoritaria se encuentra en el rechazo de los hackers al control centralizado del trabajo y al reloj capitalista que controla nuestro tiempo y reprime la creatividad del individuo. Los hackers entienden que la fuente de productividad más importante en la economía de la información es la creatividad, y no es posible crear algo interesante y valioso para la sociedad si la premura de tiempo es constante o si el trabajo se debe realizar de una forma supervisada y regulada por un horario y en un espacio de trabajo controlado, bajo una estructura centralizada.

> Aun cuando sea solamente por razones estrictamente económicas, para los hakers es importante permitir la presencia de la dimensión lúdica y de los estilos individuales de creatividad dado que, en la economía de la información, la cultura de la supervisión acaba por volverse con suma facilidad en contra de los objetivos ambicionados (Himanen, 2001: 39).

Para Himanen, esta mentalidad capitalista de la supervisión constante del trabajo y su control exhaustivo mediante un horario laboral trata a las personas adultas

como si fueran demasiado inmaduras para hacerse cargo de sus propias vidas, siendo controladas y guiadas por un reducido grupo dotado de autoridad al que se le presupone la madurez necesaria para ello. "En una cultura con este tipo de mentalidad, la mayoría de los seres humanos se hallan condenados a obedecer" (Himanen, 2001: 39).

Este control permamente en el trabajo es extrapolable a cualquier ámbito de la vida del individuo, sometido a un sistema de rutinas y de obediencia a normas y reglas impuestas por una elite autoritaria que es la que goza realmente de soberanía plena y de *legítima* autoridad. No sólo hay un control y supervisión total del trabajo, sino también del tiempo, del espacio y de la forma de ocio, de los modos de comunicarnos y de informarnos, del conocimiento divulgado, del uso de la tecnología, del consumo de bienes y servicios, de ritmos de vida predeterminados. Frente a este sistema que nos *autoriza* a disfrutar de un tiempo de ocio supeditado al tiempo de trabajo, que nos fuerza a transfigurar el tiempo de ocio en tiempo de consumo, que nos estimula al consumo masivo en un tiempo limitado en un mercado de productos y servicios reducidos, y que edita el conocimiento, emerge el libertarismo hacker. Basta recurrir al glosario hacker para entender que esta cultura se forja en ideas libertarias que describen y formulan sus alegaciones éticas: "Creemos en la libertad de expresión, en el derecho a explorar y aprender haciendo, y en el tremendo poder del individuo" (Goldstein, 2009: 268).

La cultura hacker es todo un órdago a la cultura de masas alienante y a las creencias sistémicas de que una persona emancipada que practique plenamente su libertad individual es una amenaza para el propio sistema. Y esto es lo que empuja a los poderes del Estado-nación a condenar socialmente a los hackers y a someterlos a "redadas gubernamentales, persecución selectiva, vigilancia *orwelliana* y la histeria de masas" (Goldstein, 2009: 268).

No es de extrañar, por lo tanto, que los hackers hayan sido protagonistas de numerosas piezas informativas peyorativas en los medios de comunicación dominantes —donde ha imperado el analfabetismo tecnológico (Goldstein, 2009: 198)—, en las que se expresa una profunda preocupación por los "riesgos de la adicción a la computadora" —equiparada a la heroína, la cocaína y otras drogas duras—, o por los peligros de una "propagación a través de los ordenadores" de la

mentalidad e ideales hackers, o incluso por un posible contagio de un estilo de vida en el que "se prefiere las máquinas al sexo" y en el que el individuo se despreocupa de la función reproductora (Turkle, [1984] 2005: 190) a la que la doctrina y los preceptos del cristianismo someten al ser humano. Raymond (2001) reconoce el sexo, el dinero y la aprobación social como distracciones que pueden minar la energía y diluir la pasión del hacker. Por supuesto, los hackers no son *ángeles* asexuados; tienen las mismas pulsiones que cualquier otro ser humano, pero la pasión necesaria para hackear requiere periodos de abstinencia social y sexual, y un compromiso exclusivo con la acción que se ejecuta hasta resolverla, lo cual no es óbice para el disfrute, pues la propia actividad hacker, generada por la pasión, es en sí misma una experiencia excitante y divertida que "generalmente se traduce en problemas en el mundo real", donde la "inocencia y la aventura" hackers son vistas como "el mal" y una "amenaza" (Goldstein, 2009: 7).

En la cultura hacker, pasión, diversión y goce están ligados a un alto grado de esfuerzo, dedicación, motivación y fe en la capacidad individual de aprendizaje y mejora (Raymond, 2001), por lo que cualquier agente o elemento externo es potencialmente un distorsionador. "Ser una especie de paria social ayuda a uno a mantenerse concentrado en las cosas realmente importantes, como pensar y hackear" (Raymond, 2001). En este sentido, se puede hacer una analogía con las restricciones que se imponen a los futbolistas profesionales de elite para evitar que mantengan contacto con sus familias o relaciones sexuales con sus parejas durante su participación en grandes campeonatos, como un Mundial o una Eurocopa. Concentrados en instalaciones hoteleras y deportivas, a modo de cuarteles generales, durante su periodo de participación en estas competiciones se intenta evitar que cualquier elemento distorsionador externo pueda interrumpir o alterar su concentración y menguar la energía que necesitan para alcanzar su particular trance y su objetivo extático. De igual modo, el hacker necesita aislarse para su particular trance y éxtasis.

La pasión y el goce niegan toda posibilidad de monotonía o aburrimiento, incompatibles con la actividad hacker y con cualquier arte creativo, pues el tedio es otra barrera para el hallazgo de soluciones a problemas. Raymond identifica el estado de apatía como el "mal". Sin embargo, el aprendizaje y el ensayo continuos son necesarios en el desarrollo de la actividad hacker, generando acciones aparentemente

repetitivas y aburridas a ojos de un observador ajeno a esta cultura, pero que en realidad una y otra vez se ejecutan con pasión y devoción —como el futbolista que quiere dar más y más toques a un balón sin que este caiga al suelo, con distintos movimientos y partes de su cuerpo— con el fin de adquirir una habilidad o una experiencia particular y única que lleve finalmente a la consecución de una nueva solución a un problema. "El trabajo duro y la dedicación se convertirán en una especie de intenso juego en lugar de algo monótono" (Raymond, 2001). En su manual sobre cómo convertirse en un hacker, Raymond dilucida que, "contrariamente al mito popular, no hay que ser un *nerd*[33] para ser un hacker", aunque "sí ayuda" y "muchos hackers de hecho son *nerds*". Por lo tanto, la apasionada y creativa actividad del hacker comporta también un trabajo duro, un esfuerzo que resulta necesario para crear algo mejor (Himamen, 2001: 19).

Durante la década de 1980, el nivel de paranoia colectiva sobre el mundo hacker "pareció crecer exponencialmente con el aumento de la influencia de los ordenadores y la alta tecnología en nuestra vida cotidiana" (Goldstein, 2009: 180). Los argumentos que empezaban a surgir sobre los hackers rayaban un tono apocalíptico para la humanidad y generaron preocupación, debate y contestación por algunos miembros de esta comunidad. Pero también el propio *modus vivendi* de los hackers generó un debate interno y cierta autocrítica. Por ejemplo, en agosto de 1980, la revista estadounidense *Psychology Today* publicó los llamados *The Hacker Papers*, una colección de textos comentados por el psicólogo Philip Zimbardo, recogidos del Stanford Bulletin Board, en los que varios hackers de esta universidad —una de las principales madrigueras hackers de Estados Unidos— plasmaron en un intercambio de correos sus reflexiones sobre el estilo de vida que llevaban, centrada casi exclusivamente en las computadoras, y sobre la imagen que proyectaban, aislados del resto de la vida del campus universitario, casi como inadaptados sociales. En su escrito 'Essay on Hacking', remitido a sus colegas, el estudiante Kenneth Peter —conocido en la comunidad hacker como G. Gandalf—, parece describir lo que sería una suerte de Muro de Berlín levantado para aislar al colectivo hacker del resto de la comunidad universitaria:

[33] El neoanglicismo *nerd* se ha tomado para referirse, generalmente de manera peyorativa, a individuos intelectualmente brillantes, pero con escasas habilidades sociales, que dedican gran parte de su tiempo al estudio y ampliación de conocimientos científicos y tecnológicos.

> En el centro de la Universidad de Stanford hay un gran edificio de cristal y hormigón lleno de terminales de computadoras. Cuando uno entra en este edificio a través de sus puertas de cristal, se adentra en una cultura diferente. Cincuenta personas miran pantallas de terminales. Cincuenta caras conectadas a cincuenta cuerpos, conectados a cincuenta conjuntos de dedos que golpean en cincuenta teclados finalmente vinculados a un ordenador. Si vas más adentro, se puede descubrir a los verdaderos adictos: los miembros del establishment. Estas son las personas que pasan sus vidas con las computadoras y sus compañeros «hackers». Son los miembros de una subcultura tan ajena a la mayoría de *outsiders*, que no sólo se autosegregan sino que además está segregada, a su vez, por los que no pueden entenderla. El muro es construido desde los dos lados a la vez (Peter, 1980)[34].

Kenneth Peter desarrolla a partir de ahí una descripción arquetípica del hacker, al que dibuja como un individuo brillante, "tan brillante que, de hecho, ha experimentado problemas sociales incluso antes de interesarse por las computadoras". Otros rasgos que destaca Peter son la autonomía y el gregarismo del hacker: "Muy pocos permanecen cerca de sus familias. Muy pocos se asocian con otros que no sean parte, al menos parcialmente, del grupo hacker", hasta tal punto que, según la descripción de Peter, incluso su tiempo de ocio dedicado a otras actividades no relacionadas con el *hacking* lo comparten "casi siempre con otros hackers". En tercer lugar, todos los aspectos de su existencia giran alrededor de las computadoras:

> Van a la escuela para aprender sobre computadoras, ocupan puestos de trabajo en programación y mantenimiento de computadoras, y su vida social está guiada por su relación con otros hackers. Académicamente, socialmente y económicamente las computadoras son el centro de su existencia (Peter, 1980).

Es aquí donde Peter introduce su particular autocrítica, que genera posteriormente reacciones encontradas entre sus compañeros:

> Al crear una subcultura y aislarla, estamos destruyendo la posibilidad de que las computadoras pueden ser utilizadas sabiamente como una parte integral de nuestra sociedad. Estamos excluyendo los valores humanos tan necesarios para la sabia aplicación de este logro tecnológico. Las mentes jóvenes más brillantes en nuestras mejores universidades están primero aprendiendo a jugar con juguetes que cuestan millones de dólares y luego, a cómo utilizarlos de manera constructiva. Incluso si ignoramos los costes para la sociedad en su conjunto, tenemos que mirar los costes para las personas involucradas. La computadora es un modificador de personalidades. Es altamente adictiva. Las personas que se enganchan por un período de varios meses tienden a no renunciar a ella. Y los síntomas son muy tristes (Peter, 1980).

[34] Todas la citas del texto 'Essay on Hacking' (1980), de Kenneth Peter, son traducciones propias del texto original, en inglés.

Finalmente, a modo de consejero de la comunidad, Peter alienta el debate con una serie de recomendaciones para sus colegas que sintetizamos a continuación:

- Buscar otros intereses académicos.
- Llevar un patrón de vida normal[35] para atacar la adicción a la computadora.
- Llevar una vida social equilibrada.
- Compartir emociones con otros individuos ajenos a la cultura hacker.

Por supuesto, el mensaje de Kenneth Peter desató un airado debate en el que encontró la confrontación de aquellos hackers que consideran que su actividad es una salida creativa como cualquier otra. Turkle recoge la defensa más vehemente de todas, la del científico de Inteligencia Artificial Marvin Minsky, para quien no hay diferencia entre un hacker y cualquier otra persona devota de su trabajo: "Al igual que poetas y artistas, ellos [los hackers] están comprometidos con el desarrollo de herramientas y técnicas". Respecto a la supuesta carencia de habilidades sociales de los hackers, Minsky responde con ironía situando a éstos en un escalón superior al de los psicólogos que "trivializan la condición humana en su afán de estereotipar y clasificar" (Turkle, [1984] 2005: 190).

Aunque la cultura hacker ha girado principalmente alrededor de las computadoras y de la programación, los hackers no viven exclusivamente para y por los ordenadores; viven en una cultura que crece alrededor de las computadoras pero en la que se integran áreas de conocimiento diversas, por ejemplo, las Matemáticas —otra "cultura de relativo aislamiento"—, lo que hace realmente del *hacking* "una cultura de solitarios que nunca están solos", personas comprometidas con "una ética de la tolerancia total para con todo aquello que en el mundo real sería considerado extraño" (Turkle, [1984] 2005: 196]. Raymond señala distintas destrezas vinculadas a otras artes y áreas de conocimiento como conectores con la esencia de la actividad hacker: dominio del lenguaje natural, afición a la ciencia ficción, adaptación de la disciplina

[35] Peter se refiere básicamente a normalizar horarios para comidas y descanso según los estándares establecidos en nuestra sociedad.

mental, la conciencia relajada y el autocontrol propios de las artes marciales, el estudio de disciplinas de meditación como el zen, el desarrollo de un oído analítico para la música o el gusto por los juegos de palabras y dobles sentidos. Todas estas destrezas estarían "conectadas con una mezcla de habilidades del lado derecho e izquierdo del cerebro que parecen ser importantes" para el desarrollo de la actividad hacker, ya que "tienen que ser capaces tanto de razonar lógicamente como de salirse de la lógica aparente de un problema en un momento dado" (Raymond, 2001).

Dice una canción del grupo californiano The Doors que "la gente es extraña cuando tú eres un extraño". *People Are Strange* es una crítica a la alienación social y una oda a los marginados, incluidos, por qué no, los parias sociales de los que habla Raymond: los hackers. Pero lejos de ahogarse en un estado colectivo depresivo, los hackers han presumido de su condición de seres brillantes y alegres ajenos a la triste monotonía de la normalidad. "Por esta razón, muchos hackers adoptaron la etiqueta *geek*[36] como una insignia de orgullo; es una manera de declarar su independencia de las expectativas sociales normales" (Raymond, 2001). La cultura hacker es disruptiva, por cuanto destierra normas y convenciones sociales, muchas tan banales pero tan arraigadas como la apariencia personal, lo que comemos, dónde vivimos, con quién nos relacionamos o el reparto horario y rutinario para realizar tareas y cubrir necesidades diarias, todas ellas programadas.

En la cultura hacker no hay transgresión, ni siquiera subversión, sino disrupción y alternativa a una vida reglamentada y constreñida. Las rutinas diarias y la vida monótona poco o nada tienen que ver con la cultura hacker (Mosco, 2004: 48). En la cultura hacker ni siquiera hay desobediencia, sino reivindicación de lo distinto y deserción de la ética protestante del trabajo que suministra su *ethos* al capitalismo, y de la episteme del capitalismo como marco de producción de riqueza y construcción del conocimiento. En el mundo hacker, las reglas del mundo *real* se devalúan, carecen

[36] *Geek* es un neologismo inglés que se usa popularmente para referirse a personas fascinadas por la tecnología y la informática. Su uso está muy extendido entre la comunidad de fanáticos de las tecnologías de la información y la comunicación, y a medida que la cultura dominante se ha vuelto más dependiente de la tecnología, se ha ido popularizando y extendiendo su uso. Pero sus orígenes se encuentran en referencias a comunidades consideradas marginales. El Jargon File describe así qué es ser *geek*: "Una persona que ha elegido la concentración en vez de la conformidad; que persigue la habilidad (especialmente la habilidad técnica) y la imaginación, no la aceptación social convencional. Los *geeks* suelen mostrar un alto grado de neofilia. La mayoría de los *geeks* son expertos con las computadoras y usan hacker como un término de respeto, pero no todos son en sí mismos hackers, y algunos que de hecho son hackers se llaman normalmente a sí mismos *geeks*, ya que ellos (bastante correctamente) consideran *hacker* una etiqueta que debe ser otorgada por los demás en lugar de autoasumida" (The on-line hacker Jargon File, version 4.4.7, 29 de diciembre de 2003).

de sentido y de imperativo; los dogmatismos se evaporan; el *ethos* hacker sustituye al *ethos* capitalista y el desafío del conocimiento prevalece sobre la recompensa monetaria por un trabajo dictado.

Son diversos los estudios que destacan la capacidad emancipadora del *hacking* (Himanen, 2001; Nissen, 1998; Wark, 2004) de la "jaula de hierro de la modernidad tardía y del capitalismo" (Coleman y Golub, 2008). Ese radicalismo es descrito por Jack Dann y Gardner Dozois en una recurrida analogía con el salvaje Oeste americano que previamente estableció Barlow (1990) y que Sterling (1992) identificó como el anhelo de un arquetipo cultural para los hackers que es el equivalente electrónico posmoderno del vaquero y explorador estadounidense del siglo XIX.

> Los hackers son… el tipo de espíritu inquieto, impaciente, a veces amoral o egocéntrico que roza cualquier tipo de restricción o límite, el tipo de espíritu (ya sea «libre» o «fuera de la ley», en función de cómo se mire) que se eriza con resentimiento a las leyes de otras personas, reglas, regulaciones y expectativas, e inexorablemente busca una manera de pasar por encima o por debajo o alrededor de esas reglas… En otras palabras, muy el mismo tipo de espíritu que impulsó a la gente que, para bien y para mal, abrió el Oeste americano, el tipo de espíritu que produjo sagaces exploradores, así como cuatreros, pioneros valientes y viles forajidos, y que construyeron las nuevas ciudades brillantes de los Llanos a costa de innumerables miles de vidas americanas nativas (Dann y Dozois, 1996: xiii)[37].

La idea del *Salvaje Oeste* es uno de los mitos fundacionales del ciberespacio. Esta metáfora influyó de manera decisiva en la conceptualización del espacio cíber y permitió a los primeros y más intrépidos exploradores concebirse a sí mismos en un espacio inmaterial que transgrede las intuiciones comunes basadas en lo físico sobre cómo vivir en el mundo. En este sentido, "el poder fundamental de la metáfora de la frontera es tomar como proteica una forma de comunicación como el ciberespacio y concebirla como un espacio" (Jordan 1999: 176). Una vez concebido como un nuevo espacio fronterizo, el ciberespacio está abierto a su colonización.

El mundo hacker tiene además sus "propios códigos y rituales, proporciona un marco para la vida" en una cultura que se mantiene "por la tolerancia mutua y el respeto por el individualismo radical" (Turkle, [1984] 2005: 197, 198). En la cultura hacker no existen los líderes, pero sí "héroes de la cultura y los ancianos de las tribus y los historiadores y portavoces", curtidos en "las trincheras" (Raymond, 2001). "Hay

[37] Traducción propia del texto original, en inglés.

una sociedad asociada a él, hay una cultura asociada a él y hay un estilo de vida asociado a él. Es todo un mundo", explica un senior del MIT identificado como Nick en la obra de Turkle. Obsérvese que los hackers recelan del ego y que el estatus de sabio o gurú debe ser asumido con modestia e incluso humor (Raymond, 2001); de igual modo, el "individualismo radical" al que se refiere Turkle no debemos entenderlo en la cultura hacker como oposición a las ideas de solidaridad o de cooperación, ni como sinónimo de egolatría, sino como expresión máxima de las virtudes diferenciales de un individuo que lo hacen valioso y singular para la comunidad.

> Los hackers informáticos intentan distinguirse tanto del resto del mundo como entre ellos mismos. Un hacker se involucra y se asegura de que su personalidad sea diferente a la de los demás hackers tanto como sea posible, incluso si eso significa llegar a ser algo que no es. Los hackers informáticos tienen un gran temor a ahogarse en el mar de la humanidad, todas esas caras en blanco. Por eso se mantienen apartados (Turkle, [1984] 2005: 199).

Los conceptos de cooperación, voluntariado y comunidad son básicos en la cultural hacker. Un buen ejemplo de ello fue el viaje que Kenneth Christopher 'Chris' McKinstry (12 de febrero de 1967 - 23 de enero de 2006) emprendió para enseñar computación a niños en Irak. McKinstry era un hacker canadiense, investigador en inteligencia artificial, inspirado en los ideales de Alan Touring.

En un artículo publicado en primavera de 2003 en la revista *2600*, McKinstry relataba sus intenciones en su odisea informática por Irak. Su título: 'A Hacker Goes to Iraq'. El autor describe en este texto un país prácticamente desconectado de Internet al que acudió para "enseñar" y "protestar". Sin dispositivos electrónicos, sin computadoras, incluso sin cámaras, McKinstry se introdujo en una de las zonas más calientes del planeta impulsado por su espíritu moderno y su sólida creencia en los valores de la ética hacker, sólo provisto con lápiz, papel y una copia de 1976 de *The Best of Creative Computing*, de David Ahl[38]. Su idea era enseñar computación y programación a los niños iraquíes de la misma forma que él lo había hecho en la década de 1970, con la imaginación como principal herramienta. Así lo explicaba:

[38] *Creative Computing* fue la primera revista para aficionados a la computación doméstica, creada por David Ahl.

> Iré de pueblo en pueblo y escuela a escuela enseñando sobre programación y la computadora imaginaria de Alan Turing. […] como hacker puedo traficar con una idea —la idea de la computadora imaginaria de Alan Turing— e intentar contagiar habilidad y esperanza a los niños de los pueblos (Goldstein, 2009: 619).

En los hackers hay una pulsión por enseñar, por transmitir conocimiento, por crear, construir, ayudar y colaborar, "incluso cuando no les reporte ventaja alguna y represente un serio riesgo personal" (Sterling, 1992). "Los hackers resuelven problemas y construyen cosas, y creen en la libertad y la ayuda mutua voluntaria" (Raymond, 2001). Pero para la solución de problemas es necesario compartir experiencias sin desgastarse en la reinvención de lo que ya existe y funciona. Por ello, el hacker debe conducir sus tareas por los caminos de la operatividad, el pragmatismo, la cooperación y la inteligencia colectiva (Sádaba Rodríguez y Roig Domínguez, 2004). "Los cerebros creativos son un valioso recurso limitado. Estos no deben desperdiciarse reinventando la rueda cuando hay tantos problemas nuevos fascinantes esperando ahí fuera", clarifica Raymond en su venerado texto *How to Become a Hacker* (2001). Los hackers también se distinguen del resto de la sociedad en su concepción de la transferencia de conocimiento. Sus publicaciones están al margen de la mercantilización del saber.

> Para comportarte como un hacker debes creer que el tiempo para pensar que emplean otros hackers es precioso, tanto, que es casi un deber moral para ti compartir la información, resolver problemas y luego revelar la solución para que otros hackers puedan resolver nuevos problemas en lugar de enfrentarse perpetuamente a los viejos (Raymond, 2001).

Los primeros hackers del Massachusetts Institute of Technology, por ejemplo, publicaron sus más poderosas técnicas en 1972 en un documento llamado *HAKMEM*. En una cultura suscrita a la mercantilización del conocimiento, un documento de tal envergadura intelectual podría haber sido el comienzo de una revista, de una publicación periódica, de un producto comercial, de un servicio académico, pero no estaba en la naturaleza de los primeros hackers hacer algo tan oficial o académico (Turkle 2005: 208). Y así fue cómo este documento adquirió valor de mito en la literatura hacker.

Sin embargo, es necesario aclarar que la transferencia de conocimiento hacker no está en contradicción con el ánimo de lucro si éste no implica una traición a la

comunidad y a la pasión, el entusiasmo, la libertad y la creatividad con la que opera el hacker:

> No tienes que creer que estás obligado a donar *todo* tu producto creativo, aunque los hackers que lo hacen son los que obtienen más respeto por parte de otros hackers. Es congruente con los valores hackers vender lo suficiente de ello para alimentarte, pagar el alquiler y mantener tus computadoras. Está bien utilizar tus habilidades de *hacking* para mantener una familia o incluso hacerte rico, siempre y cuando no olvides tu lealtad a tu arte y a tus compañeros hackers mientras lo haces (Raymond, 2001).

Todo esto es, en definitiva, una lucha contra la homegeneización y estandarización del modelo social del capitalismo, donde se nos prometen ciertas seguridades y garantías tangibles e intangibles, y la ilusión de un *yo* inalienable y soberano, a cambio de la paradoja de formar parte de una masa compacta en la que perdemos nuestras identidades singulares. El modelo de trabajo, el estilo de vida, incluso el modelo educativo del sistema capitalista, nos convierten en seres anodinos. Es sólo con el ejercicio libre de la creatividad pasional cuando el individuo se diferencia de la masa y hace emerger su *yo* diferencial y sustancial. Por ejemplo, "a ojos del hacker, los lenguajes [de programación] comerciales, como los lenguajes FORTRAN y COBOL de IBM, y el lenguaje «científico» PASCAL representan la uniformidad de la cultura de masas que entierra al individuo en la multitud" (Turkle, [1984] 2005: 209).

Para Hannemyr (1999), "la aparición de los hackers como un grupo identificable coincide estrechamente en el tiempo con la introducción de diversos métodos *tayloristas* en el desarrollo de software". Los principios y tácticas *tayloristas* aplicados al desarrollo de software y hardware son rechazados por los hackers, contrarios a la planificación, ordenación, jerarquización y mecanización de un trabajo que debe ser un arte y un oficio. Frente al nuevo obrero fabril que configura la industria digital *taylorista*, los hackers reivindican al artesano que preserva el control sobre todo el proceso de trabajo y el conocimiento mediante el acceso libre al código fuente y su libre uso. Con su ética, los hackers se enfrentan al *taylorismo* digital, que "fomenta la segmentación del talento reservando el permiso para pensar a una pequeña elite de empleados encargados de llevar adelante el negocio, funcionando junto con otros trabajadores igualmente cualificados en más puestos de trabajo *taylorizados*"

(Brown, Lauder y Ashton, 2011: 81)[39].

El *hacking* es una respuesta a lo que Featherstone (1988: 203) describe, en el contexto de la posmodernidad, como el declive de la originalidad y del genio del productor artístico y a la suposición *pop* de que el arte sólo puede ser repetitivo. Meyer y Thomas (1990) encuadran el *hacking* en las formas *positivas* del posmodernismo que constituyen un ataque intelectual a lo que Newman (1985) explica como una cultura de masas atomizada, pasiva e indiferente en un ambiente posmoderno de inflación del discurso que, principalmente, recorre las esferas de la cultura y de la comunicación. Meyer y Thomas justifican así la explicación del *hacking* como manifestación posmodernista positiva:

> Es este estilo de rebeldía juguetona, la subversión irreverente y la yuxtaposición de la fantasía con la realidad de alta tecnología son lo que nos impulsa a interpretar el *underground* informático como una cultura posmodernista (Meyer y Thomas, 1990: 9).

En la cultura hacker hay libre albedrío, el entusiasmo da rienda suelta a la pasión y a la creatividad, se construye un culto a la originalidad y a la destreza para resolver problemas —incluso el más absurdo o aparentemente insignificante problema— o para mejorar constantemente procesos y sistemas cada vez más complejos y eficientes. Esta búsqueda continua de mejoras implica cambios permanentes y esa mutabilidad constante, anárquica e incontrolada genera desconfianza, temor, inseguridad —si no está controlada, reglamentada, programada y calendarizada por fuerzas institucionalizadas— en aquellos individuos, colectivos, organizaciones e instituciones acomodados en el discurso de una sociedad, la capitalista, cuyos valores más ensalzados desde los púlpitos del poder han sido la *seguridad* y la *estabilidad*, principios que han ordenado nuestra realidad tras las dos grandes guerras mundiales del siglo XX y las grandes depresiones económicas en Estados Unidos y Europa. Sin embargo, las sociedades informacionales estructuradas por el capitalismo tecnológico requieren, paradójicamente, generar ambientes líquidos con un alto grado de mutabilidad y de obsolescencia en el mercado para *asegurar* su *estabilidad*. Nótese, por ejemplo, cómo las actuales grandes compañías tecnológicas han tomado para sí la praxis hacker y la han transformado y adaptado a sus intereses

[39] Traducción propia del texto original, en inglés.

económicos, haciendo de las mejoras constantes una obligación para sus departamentos de desarrollo y una oportunidad comercial sin precendentes en la historia de las sociedades capitalistas, generando en las masas consumidoras globales necesidades impuestas por el márketing que se aproximan a lo que podríamos llamar un sistema tecnológico de dictadura emocional: el consumidor queda atado emocionalmente a una tecnología en constante desarrollo y a cuyas constantes innovaciones programadas sólo puede acceder pagando altos costes económicos y emocionales en intervalos de tiempo cada vez más cortos. El capitalismo tecnológico ha —permítasenos la redundancia— acelerado el principio de aceleración de John Maurice Clark:

> La «ley de aceleración continua» de Clark obliga a lanzar los productos tecnológicos cada vez más deprisa. El capital de los empresarios que alcanzan el éxito en este campo tiene que desplazarse también mucho más deprisa que antes. Las inversiones cambian con frecuencia los objetivos en el plazo de horas, minutos o incluso segundos. Al capital no le está permitido estancarse en almacenes o en personal superfluo: tiene que estar disponible para una rápida inversión en innovación tecnológica o en objetivos constantemente permutables en el seno de los mercados financieros (Himanen, 2001: 23).

A la obsolescencia técnica programada se ha unido ahora otro tipo de obsolescencia, de índole emocional, en una estrategia de abastecimiento continuo, ininterrumpido, de nuevos productos tecnológicos con licencias privativas que se suceden rápidamente en versiones mejoradas de un mismo modelo en apenas unos pocos meses. A la primera versión 1.0 de un dispositivo tecnológico la suceden versiones mejoradas de su anterior en tiempos extremadamente reducidos, cada vez más cortos. El mercado tecnológico transnacional encuentra perfecto acomodo en un nuevo entorno capitalista de rápida caducidad —todo es breve, fugaz, inestable, líquido: trabajo, información, productos, identidades, etc.—, donde el objetivo último es acelerar el capital acelerando el consumo; el hiperconsumo es consecuencia de la aceleración en el abastecimiento de nuevas versiones de un mismo producto con una caducidad emocional cada vez más corta, sin esperar a que su punto de obsolescencia mecánica programada siquiera se aproxime. Se produce un *continuum* de nuevas versiones que van excluyendo a sus predecesoras[40].

[40] En el Capítulo III veremos que, de forma análoga, también los medios de comunicación abastecen los

Basta un pequeño cambio de diseño, una nueva funcionalidad, una leve mejora o una actualización de sistema para que el último iPhone o iPad o el último modelo de teléfono inteligente de Samsung se conviertan en objetos emocionalmente obsoletos para los usuarios de un día para otro. La estrategia se culmina con campañas transmediáticas globales de márketing. La presentación de un nuevo modelo de iPod, iPhone o iPad de Apple es todo un acontecimiento mundial. El nuevo modelo se presenta en red, en múltiples medios, formatos y soportes: una conferencia en *streaming*; los asistentes comparten fotografías, vídeos, opiniones, comentarios y enlaces en tiempo real en las redes sociales en línea; los medios de comunicación tradicionales son fagocitados por el departamento de márketing de la compañía de la manzana y disfrazan como información periodística colosales publirreportajes sobre la marca y su novedad comercial; blogueros de todo el planeta quieren ser los primeros en tener las primeras imágenes del dispositivo, o el propio aparato en mano, para escribir las primeras críticas y análisis, y aparecer en lo más alto del ránking de búsquedas en Google, pero también lo más arriba en la pirámide social, pues poseer antes que otros el último modelo de un iPhone confiere un estatus elitista y cierta gloria social; cientos de vídeos sobre el nuevo modelo se suben a YouTube en pocas horas; calles, canales de televisión y de radio, periódicos, revistas y páginas de Internet se llenan de la creatividad publicitaria que anuncia la enésima *revolución* tecnológica, otro cambio dramático en la comunicación humana, sin apenas tiempo para asimilar la anterior. La necesidad está creada y hay que satisfacerla. Se produce un éxtasis colectivo embriagador.

La emoción y deseo de posesión que produce un nuevo modelo de un producto tecnológico convierte a su antecesor en un aparato obsoleto y sin brillo social. Es la obsolescencia emocional programada. La compra —dice el teórico tecnológico Tom Chatfield— deja de ofrecer la gratificación por la que fue adquirido: "Como el autor (y compañero columnista de BBC Future) Matt Novak señaló en Twitter cuando Apple presentó su cuarta generación del iPad […]: «la verdadera historia aquí es que Apple acorta su ciclo de obsolescencia planificada a seis meses»"[41] (Chatfield, 2014)[42].

nuevos hipermercados de la información con contenidos fugaces que se suceden a velocidades desorbitadas.

[41] Novak, M. [paleofuture]. (2012, Oct 23). Forget the miniPad. The real story here is that Apple shortened its planned obsolescence cycle to 6 months. [Tweet]. Recuperado de: https://twitter.com/paleofuture/status/260802228284166144.

[42] Las citas atribuidas a Tom Chatfield fueron traducidas del texto original, en inglés, por el autor de esta

El sistema capitalista necesita convertir deseos humanos en necesidades, descontextualizando las emociones de su finalidad. Para que se produzca el hiperconsumo se necesitan emociones rápidas, instantáneas y efímeras; emociones líquidas. Satisfecha una emoción, se va en pos de otra y otra y otra, en una vorágine imparable que ataca a todos los estratos sociales. El único objetivo es un consumo constante y cada vez más rápido que acelere el capital, y la vía elegida es la mercantilización de las emociones: las experiencias emocionales se pueden comprar con dinero. "Lograr un avance técnico revolucionario varias veces al año es un plan de negocio imposible. Alimentar un frenesí público en el mismo intervalo de tiempo, sin embargo, es eminentemente posible", arguye Chatfield.

La tecnología, dice Turkle (2012: 1), "es seductora cuando lo que ofrece conecta con nuestras vulnerabilidades humanas". En medio del fulgor tecnológico que estamos experimentando, se articula un sistema de gratificaciones puramente emocionales: ya no valoramos la tecnología por su funcionalidad, sino por las emociones que genera poseer cierta tecnología y la falsa creencia de pertenencia a una vanguardia social. Todo es ilusorio y fugaz. Lo que hacemos con los dispositivos móviles ya no es el factor clave; mucho más importante es lo que proyectamos a través de la tecnología, la forma en que la posesión de esta tecnología nos hace sentir y nos sitúa: no importa qué podemos conseguir técnicamente con ocho megapíxeles más de resolución en la cámara del *smartphone*, sino el acto de presumir de la mejor resolución del mercado, apenas por unos meses.

Nuestro acceso a la tecnología determina el modo en que somos percibidos por los demás y, por consiguiente, el estatus social y cultural que en apariencia ocupamos.

> El iPad es el paradigma de un cambio sutil en la industria de la tecnología que tiene un único objetivo: conseguir que los consumidores compren más y más rápido. Todo es parte de un cambio en la tecnología, que se ha desplazado gradualmente de un énfasis en la utilidad a la santa trinidad de hoy de la apariencia, sensación y estilo de vida. Un cambio iniciado por Apple, pero cada vez más defendido por todas las empresas de alta tecnología, que se inspira en la moda, posicionando tabletas, computadoras y software como faros culturales: sellos que dicen de inmediato quién eres o, más bien, qué aspiras a ser (Chatfield, 2014).

En el lado opuesto, la plataforma colaborativa Wordpress toma y respeta de la cultura hacker sus principales valores. Wordpress es un software libre bajo licencia de

---

tesis.

código abierto GNU General Public License, de la Free Software Foundation, sobre el que se sostienen en Internet millones de páginas web. En concreto, se trata de un sistema de gestión de contenidos en línea —conocidos popularmente por sus siglas en inglés, CMS (Content Management System)—, desarrollado en lenguaje PHP para entornos que ejecuten MySQL y Apache. Como se señala en la propia página de Wordpress.org, esta licencia tiene unas "implicaciones políticas y filosóficas" basadas en razones pragmáticas e idealistas vinculadas a la cultura hacker. La licencia otorga absoluta libertad a cualquier persona para descargar o copiar gratis el paquete completo de Wordpress, instalarlo, modificarlo y redistribuir su código fuente. En el preámbulo de esta licencia, la propia Free Software Foundation aclara:

> Las licencias para la mayoría del software y otros trabajos prácticos están diseñados para quitarle su libertad de compartirlo y modificarlo. En cambio, la Licencia Pública General GNU pretende garantizarle la libertad de compartir y modificar todas las versiones de un programa, para asegurarse de que el software permanece libre para todos sus usuarios. Nosotros, la Free Software Foundation, usamos la Licencia Pública General GNU en la mayor parte del software de la Free Software Foundation, y se aplica también a cualquier otro trabajo liberado de esta manera por sus autores. Usted también puede aplicarla en sus programas (Free Software Foundation, 2007)[43].

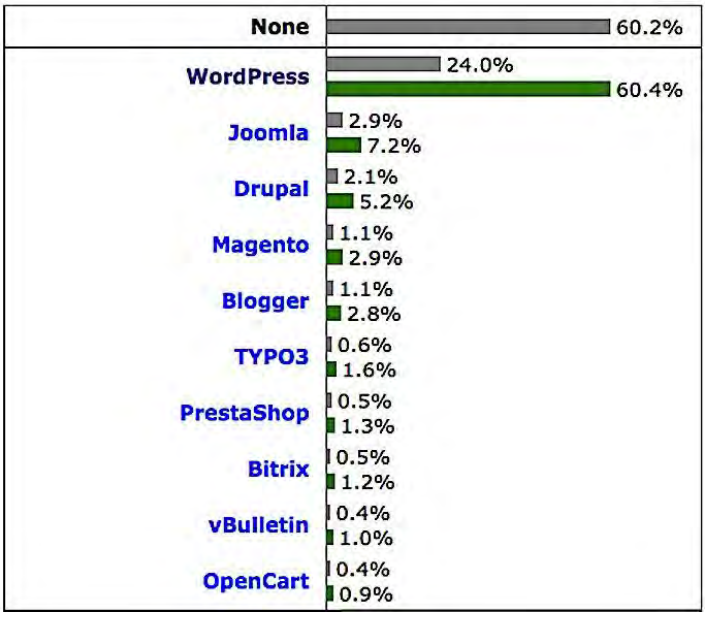
Para garantizar que se cumple con su política de uso y proteger los derechos de los usuarios, la Free Software Foundation establece una serie de condiciones que "prohíban a cualquiera negarle a usted estos derechos o pedirle que renuncie a los mismos". De este modo, quien distribuye copias de programas de este tipo, ya sea gratuitamente o por una tarifa económica, debe transferir a los receptores todos los derechos que tiene el distribuidor sobre el programa, asegurándose de que reciben o pueden conseguir el código fuente. Y debe mostrarles estos términos de forma que conozcan sus derechos. La licencia garantiza tanto la protección de los derechos de autor del software como la copia, distribución y/o modificación legal del software, e insta a quienes ejecuten modificaciones a informar sobre las mismas para que el receptor conozca las diferencias entre el código original y el modificado, para que cualquier problema introducido por otros no afecte a la reputación de los autores originales. Por último, sabedores de que cualquier programa libre está constantemente amenazado por las patentes de software, y para evitar el peligro de que los

[43] Traducción propia del texto original de la Free Software Foundation, en inglés.

redistribuidores de un programa libre obtengan patentes por su cuenta, convirtiendo el programa en privativo, cualquier patente debe ser solicitada para uso libre de todos los usuarios, para garantizar los principios hackers en los que se fundamenta esta licencia.

Según datos recogidos el 12 de junio de 2015 de W3Techs.com (Web Technology Surveys)[44], el 24 por ciento de los sitios web en el mundo usan Wordpress incluidos la revista estadounidense *Time* y los blogs del periódico español *ABC*.

Tabla 2: Sistemas de gestión de contenidos *online* más populares.



Fuente: http://w3techs.com/technologies/overview/content_management/all.

Frente al usuario de tecnología libre, el autoproclamado *usuario* de tecnologías comerciales nunca fue autónomo y verdaderamente participativo; sigue siendo un mero receptor y consumidor sin identidad propia, que actúa con la característica pasividad que se le asigna e impone al sometido, ahora en un mercado de masas transfronterizo, global y abrumador. Pero sí es usario autónomo en el mundo hacker, donde la innovación y la mejora es un acto abierto, transparente, participativo y colaborativo, que ni se mercantiliza ni se programa en el calendario.

En el *mundo* Apple, el *éxito* no es *real*, sino percibido en una cultura del materialismo. El *éxito* es sinónimo de lucro económico y de fama mediática y ciberespacial, pero sólo una elite dirigente acapara el reconocimiento social dervivado

[44] W3Techs actualiza a diario los datos recogidos de sitios web, excluyendo las URL de páginas web individuales, subdominios y dominios redirigidos a otras direcciones. Las estadísticas se elaboran con datos obtenidos de los diez millones de sitios web más importantes del mundo.

de la venta de unas mejoras que son opacas, herméticas, impuestas como obligación laboral a sus desarrolladores, y que se comunican y entregan de arriba abajo en un modelo piramidal: primero, a una elite económica y tecnológica, y posteriormente, a los distintos estratos sociales, que van accediendo a estos avances tecnológicos de manera progresiva —según su posición en la pirámide—, a medida que el producto va quedando aparentemente obsoleto por la aparición de nuevas versiones o modelos que devalúan su valor monetario y emocional en el mercado.

En el *mundo* hacker, sin embargo, las mejoras son transparentes, abiertas, accesibles, horizontales, libres y pasionales; no están motivadas por un ánimo de lucro, sino por un espíritu inquieto por resolver problemas, compartir soluciones —y, por lo tanto, liberar la información— y, en última instancia, la gratificación es el reconocimiento de la comunidad, en la que todos conocen y aprecian los logros de cada individuo (Himanen, 2001: 51). En el *mundo* hacker el *éxito* se traduce en "creer en algo, no comprometer tus ideales y estar en paz con uno mismo" (Goldstein, 2009: 269).

> La filosofía de este movimiento [hacker] que nace ligado al mundo del software y al desarrollo de las redes choca desde un primer momento con dos dinámicas: la del Estado que impone su necesidad de regularizar el nuevo fenómeno (todo nuevo fenómeno) y la del mercado que pretende hacer valer en el terreno de la creatividad y la investigación científica sus principios de propiedad y su pulsión mercantilizadora sobre todo nuevo ámbito de producción. Desde sus orígenes la comunidad hacker entendió la generación de código ejecutable (software) como un fenómeno comunicativo: el software es información y la información generada por el conocimiento colectivo de la comunidad investigadora ha de fluir libremente, fuera de las limitaciones mercantiles y estatales (Sádaba Rodríguez y Roig Domínguez, 2004).

Esa tensión entre ambas culturas —la lucha de fuerzas entre el idealismo hacker y el materialismo capitalista— fue anticipada y plasmada en *Software Wars*, un texto escrito en 1978 por el hacker de la Universidad de Stanford Mark Crispin[45] y compartido en la lista de correo electrónico dedicada a ciencia ficción que mantenían entonces algunos hackers aficionados a este género.

Software Wars es una adaptación hacker libre y breve de *Star Wars* inspirada por el cortometraje paródico *Hardware Wars* (1978), de trece minutos, dirigido por

[45] Todas las citas del texto original, en inglés, de Mark Crispin fueron traducidas por el autor de esta tesis.

Ernie Fosselius[46]. En la obra de Crispin, la tensión entre el *bien* y el *mal* —la Fuerza y el Lado Oscuro— es llevada al campo de las computadoras, donde, obviamente, la cultura hacker representa el bien y los burócratas, ingenieros y programadores del lado del mercado son la encarnación del mal. En la introducción de su relato, Crispin describía ese escenario bipolarizado, en el que los hackers son poseedores de un poder místico, el *hack*:

> Hace mucho tiempo y muy lejos, la galaxia de procesamiento de datos era regida por las siniestras fuerzas del Imperio PASCAL. Años atrás, lo había sido por la República del Hacking, donde todos los lenguajes de programación y programadores vivían juntos en paz y armonía. La tierra de la República era patrullada por los Wizards, expertos en todas las formas de magia, que a diario daban a conocer nuevos milagros para maravilla de los ciudadanos de la República. Dibujaron sus poderes místicos del Hack, que era su auxilio en cualquier dificultad (Crispin, 1978: 2).

Nada anecdótica es la referencia que esta fábula dedica a *HAKMEM* —el documento publicado por los hackers del MIT en 1972— cuando Moby Foobar (una suerte de héroe hacker mitológico cercano al personaje del maestro Yoda) se lo entrega al protagonista de esta historia, Fluke (el Luke Skywalker de los hackers):

> Esta es *HAKMEM*, una elegante herramienta de programación de una era más civilizada. Un experto en el Hack podría obrar milagros de programación con ella, mejorar el tiempo de respuesta y ser invitado a todas las buenas fiestas. Aquí. (Crispin, 1978: 9).

El *hack*, en definitiva, se identifica con un poder divino, con una fuerza omnipotente y omnipresente. "El Hack es lo más querido y cercano a los corazones de todos los magos. Es lo que le da al mago su poder. El Hack está en todas partes y es parte de todo" (1978: 9)

Lo que describe el autor es un enfrentamiento entre dos bandos, dos culturas de la computación que dirimen una guerra civil en la que los hackers actúan como rebeldes[47] contra el Imperio:

> Al comenzar nuestra historia, la guerra civil ha estallado. Hackers rebeldes, atacando desde una base de datos oculta, han ganado una victoria sorpresa contra el Imperio. En el curso de la batalla, los espías rebeldes se apoderaron de copias del

[46] *Hardware Wars* fue la primera paraodia de *Star Wars*, su producción costó unos 8.000 dólares y se convirtió en un éxito, recaudando más de un millón de dólares.

[47] La rebeldía parece una condición connatural al hacker. Como veremos a lo largo de este trabajo, hackers y hacktivistas se posicionan como disidentes y, por tanto, como rebeldes contra el poder y las normas establecidas.

> diseño de la DÉCIMA ESTRELLA del Imperio, su nuevo procesador y sistema operativo (1978: 2).

Es la idealización del hacker como "rebelde, enemigo de las instituciones y de la conformidad, defensor de la idiosincrasia, la individualidad, el genio y el culto al individuo" (Turkle, [1984] 2005: 210). Misticismo, magia, fuerza y mitología envuelven esa rebeldía y disidencia en el gran relato de la comunidad hacker (Goldstein, 2009: xxxvii). Sus mentes, dice Turkle, deben estar libres para volar, inventar y superar los límites que imponen las fuerzas institucionalizadas, cuyos "registros" y "estructura" empujan a la muerte espiritual del individuo. De la lectura de Turkle se desprende que los tres principios básicos del *ethos* original del *hacking* son:

1. Simplicidad: el acto debe ser sencillo pero con un resultado impresionante.
2. Maestría: el dominio del acto implica un conocimiento técnico sofisticado.
3. Ilicitud: el acto es contra las reglas.

La ilicitud en la que incurre el auténtico hacker no es delictiva, por cuanto no busca causar daño. A finales de julio de 1991, un grupo de hackers holandeses accedió a los sistemas informáticos militares de Estados Unidos. Uno de los episodios fue capturado en vídeo por la revista *2600* y parte de éste se emitió en un programa de televisión de ámbito nacional, en Estados Unidos. Los responsables de la revista hacker decidieron distribuir también el vídeo por su propia cuenta, para que más personas fuesen testigos de cuán vergonzosamente fácil era conseguir acceso a las computadoras militares. El propósito de la acción de los hackers holandeses no era dañar ningún sistema militar, sino demostrar lo fácil que sería hacerlo. Se tuvo mucho cuidado para asegurar que no se produjese ningún daño o alteración de los datos en el sistema accedido. Ningún secreto militar fue filtrado y ningún dato fue guardado por los hackers. Aquella acción fue una advertencia de la existencia de agujeros de seguridad en los sistemas informáticos del Ejército estadounidense.

Otro caso llamativo fue el ocurrido en Reino Unido en el verano de 1994, cuando un hacker logró entrar en las bases de datos de la compañía British Telecom. El caso fue destapado el 24 de noviembre de aquel año por el periódico *The Independent* como "un escándalo" sin precedentes en Reino Unido que comprometía los laxos sistemas y métodos de seguridad del país.

Así describía el diario británico el caso de este hacker, que se infiltró en British Telecom por medio de un contrato temporal de trabajo y accedió a miles de datos secretos con "asombrosa facilidad":

> Números de teléfono y direcciones para el MI6 y el MI5, muchas instalaciones secretas del Ministerio de Defensa y otros datos muy sensibles fueron copiados desde la computadora por el hacker sin ningún conocimiento técnico especial. El material se envió a Internet, una red mundial de computadoras, donde cualquiera de sus 35 millones de usuarios tendría acceso potencial a éste (Kelsey, 1994).

Las miles de páginas con documentos confidenciales habían sido enviadas por un informante anónimo al periodista escocés Steve Fleming, a través de Internet. Entre los datos se incluían también registros del Cuartel General de Comunicaciones del Gobierno —el GCHQ (Government Communications Headquarters)—, en Cheltenham; domicilios de militares de alto rango; detalles de instalaciones telefónicas para la estación de comunicaciones secretas de Estados Unidos en Menwith Hill, en North Yorkshire; información sobre el búnker en Wiltshire para refugiar al Gobierno británico en caso de una guerra nuclear; la ubicación de bases de misiles y centros de mando y control militar en el Reino Unido; los números de línea privada de John y Norma Major en Downing Street; las líneas privadas del Palacio de Buckingham y del Palacio de Kensington, y datos de la ubicación de una serie de edificios de servicios de inteligencia en Londres.

Al dejar en evidencia los sistemas de seguridad y dirigir la atención pública a sus vulnerabilidades, los auténticos hackers no sólo ridiculizan a las autoridades y a las grandes corporaciones, también alertan a la sociedad de que datos sensibles referidos a su seguridad y privacidad están en manos negligentes, y nos advierten de que los sistemas deben ser mejorados para que no puedan infiltrarse en ellos auténticos delincuentes (Goldstein, 2009: 254, 255, 558).

I.2.1. Hackers *vs* crackers

La criminalización de los hackers diseñada por el Estado-nación, diseminada por los medios de comunicación de masas e inoculada en la población, se fundamenta en una arbitraria identificación de los miembros de esta comunidad como *crackers*, "los usuarios destructivos cuyo objetivo es crear virus e introducirse en otros sistemas" (Himanen, 2001: viii). A diferencia de los *crackers*, "en todo el mundo, los hackers han utilizado sus habilidades tecnológicas para realizar intervenciones encaminadas a resolver crisis en sus entornos", hasta el punto de convertirse en "nuevos héroes" civiles (Shah, 2011).

Según el Jargon File, el término *cracker* fue acuñado por los hackers en 1985 para defenderse del "mal uso periodístico" de la palabra *hacker*. Su uso denotaba la repulsa de esta comunidad al robo y al vandalismo *cracker*. Esto no implica que los hackers se deban abstener de introducirse en sistemas sin permiso, pero siempre debe hacerse con un espíritu juguetón y curiosidad, y por razones justificadas que no conlleven destrucción o daño alguno. Por ejemplo, se justifica que un hacker se adentre en un sistema informático ajeno para demostrar sus fallas de seguridad. Pero los esfuerzos de los hackers por desligarse de los *crackers* han sido tan intensos y constantes como infructuosos. La lucha contra el poder institucionalizado ha sido hasta ahora en vano. Los medios de comunicación dominantes mantienen la palabra *hacker* asociada casi exclusivamente a delitos informáticos, una práctica que hace "comprensible" el malestar que este uso perverso de la palabra genera en la comunidad hacker, por suponer un "ataque a sus valores implícitos" (Sterling, 1992).

La literatura hacker apenas ha alcanzado a la propia comunidad y a algunos investigadores y curiosos que han querido conocer las raíces de esta cultura, mientras una mayoría, la masa, ha sido *infotoxicada* por los aparatos dominantes de diseminación semántica del Estado-nación: prensa, radio, TV, diccionarios, informes institucionales y corporativos, etc. han impedido distinguir la ética hacker de la perversidad *cracker*:

> Los auténticos hackers […] no quieren tener nada que ver con ellos. Los hackers reales piensan mayormente que los crackers son perezosos, irresponsables y no muy brillantes, y objetan que ser capaz de romper la seguridad [de un sistema] te convierta en un hacker […]. La diferencia básica es esta: los hackers construyen cosas, los *crackers* las rompen (Raymond, 2001).

Esta diferenciación entre hackers *auténticos* y *crackers* se origina en la propia comunidad hacker para contrarrestar el estereotipo negativo que han difundido los medios. "El primer nombre está reservado a usos creativos que contribuyen a proyectos de software socialmente útiles. Las connotaciones negativas del crimen informático están reservadas para el último grupo" (Söderberg, 2009: 94)

Para Eric S. Raymond, desafortunadamente muchos periodistas y escritores han sido engañados en el uso de la palabra *hacker* para describir a los *crackers*; un engaño articulado por los aparatos de poder del Estado-nación y las grandes corporaciones tecnológicas, interesadas en criminalizar a una comunidad que cuestiona su hermetismo y un modelo comercial privativo y tirano que deja al consumidor en manos de la tecnología, en la más absoluta ignorancia e indefenso, y a la sociedad en general, impedida por barreras técnicas, legales o institucionales (como las del software de código cerrado) que evitan la reutilización y mejoras comunitarias, y nos fuerzan a reinventar la rueda una y otra vez (Raymond, 2001).

La obsesión por desligar a los hackers del ámbito criminal está presente en prácticamente toda la literatura de naturaleza hacker. Himanen (2001), por ejemplo, también acusa a los medios de comunicación de haber usado perversamente la palabra *hacker*, desde mediados de la década de 1980, para referirse a los delincuentes informáticos, lo que empujó a los auténticos hackers a empezar a usar la palabra *cracker* para identificar a los piratas o delincuentes informáticos, con el fin de evitar la confusión.

El uso perverso de la palabra *hacker* es una manipulación informativa, una distorsión de la realidad, un engaño al ciudadano, un fraude semántico que mantiene por cuatro décadas la leyenda de que los hackers son criminales (Goldstein, 2009: 266).

> Lo que la prensa no alcanza a ver es la distinción entre el *hacking* que se hace por aventura y el uso de conocimientos hackers con fines de lucro personal. Para ellos todo es lo mismo. Alguien que vende códigos telefónicos es igual que alguien que manipula la red telefónica de manera salvaje e imaginativa. Mediante la definición de los dos como uno y lo mismo, en realidad podríamos estar siendo empujados hacia comportamientos criminales, ya que es lo que se espera de nosotros (Goldstein, 2009: 267).

Ilustración 2: Ejemplo de mal uso de la palabra *hacker* en *El País*.

Fuente: captura de pantalla tomada de la edición digital de *El País*.

Un caso paradigmático de manipulación informativa sobre los hackers —o de pura ignorancia y negligencia periodísticas— se produjo durante la guerra del Golfo en la década de 1990, cuando medios de comunicación tradicionales contribuyeron a popularizar la creencia de que hackers holandeses se habían introducido en sistemas informáticos militares y habían ofrecido información secreta a Sadam Husein, información con la que supuestamente podría haber ganado la guerra de Irak.

> No hubo evidencias. No hubo hechos. Sólo un chiflado con aires de autoridad y el deseo de los medios de conseguir otra historia sensacionalista. Repetida suficientes veces, este tipo de basura se convierte finalmente en realidad y la inevitable reacción contra la «crisis» se acepta como necesaria. Todos lo sabemos, pero se sigue haciendo una y otra vez (Goldstein, 2009: 544).

A los hackers no sólo les ha preocupado clarificar las diferencias entre ellos y los auténticos delincuentes informáticos; la persecución policial y mediática a la que han sido sometidos también les empujó desde tiempos tempranos a denunciar con vehemencia los abusos del sistema institucionalizado. El 8 de enero de 1986, uno de los hackers más reputados del mundo, Loyd Blankenship —más conocido por el pseudónimo The Mentor, miembro destacado de la segunda generación del grupo hacker estadounidense Legion of Doom—, publicó en la revista *Phrack*, tras una detención policial, un texto que se convirtió en uno de los manifiestos de culto entre los miembros de esta comunidad y piedra angular de esta cultura: *The Conscience of a Hacker*. Los tres últimos párrafos de esta breve apología del *ethos* y la ética hacker evidencian la frustración que los mecanismos del sistema institucional generan en los hackers:

> Este mundo es nuestro... el mundo de los electrones y los interruptores, la belleza del baudio. Utilizamos un servicio ya existente sin pagar que podría haber sido más barato si no fuese por esos especuladores insaciables. Y nos llamáis delincuentes. Exploramos... y nos llamáis delincuentes. Buscamos ampliar nuestros conocimientos... y nos llamáis delincuentes. Existimos sin color de piel, ni nacionalidad, ni religión... y vosotros nos llamáis delincuentes. Construís bombas atómicas, hacéis la guerra, asesináis, estafáis y nos mentís tratando de hacernos creer que es por nuestro bien, y aún nos tratáis como delincuentes.
>
> Sí, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis.
>
> Soy un hacker, y este es mi manifiesto. Podéis parar a este individuo, pero no a todos... después de todo, somos todos iguales. (The Mentor, 1986)[48].

Legion of Doom se había formado, según sus propios fundadores, para reunir a las mejores mentes del *underground* de la computación; en ningún caso su intención era causar daños o lucrarse. Su única motivación era compartir experiencias y debates sobre computación. The Mentor lo justificaba así tras la redada masiva de hackers de 1990 en la operación *Sun Devil*[49]: "El grupo siempre ha mantenido los más altos estándares éticos... En muchas ocasiones hemos tomado medidas para evitar el abuso de sistemas […] El mayor crimen que se ha cometido es el de la curiosidad" (Goldstein, 2009: 497).

Pese a insistir en las bondades de sus actos, el 16 de noviembre de 1990 tres de sus miembros fueron condenados en Atlanta (Georgia, Estados Unidos): Robert Riggs (The Prophet), Frank Darden Jr. (The Leftist) y Adam Grant (The Urville). Los tres fueron declarados culpables de varios cargos de piratería informática, en particular relativos a la SBDN (la Red de Datos de Southern Bell, operada por Bell South). Supuestamente, Riggs había accedido a la SBDN y fue quien envió el famoso documento del sistema E911 a Craig Neidorf para su publicación en *Phrack*.

Neidorf se libró de la cárcel tras cerrarse el caso por falsedad de información aportada por Bell South; tampoco se demostró que la incursión en el sistema de Bell hubiese causado daño alguno. Sin embargo, los tres hackers de Legion of Doom ya se habían declarado culpables de haber accedido a la computadora de Bell South y fueron finalmente condenados: Riggs, a 21 meses en prisión y sus otros dos compañeros, a 14 meses cada uno y multa para los tres de 233.000 dólares. Entre la comunidad hacker

[48] Traducción propia del texto original, en inglés.
[49] Ir a página 155.

fueron conocidos como "Los Tres de Atlanta".

Este caso evidenció, por un lado, la negligencia de una gran compañía telefónica como Bell South al dejar abiertas puertas de su sistema de datos y, por otro lado, la incapacidad de las autoridades para entender y manejar el *hacking* informático y sus motivaciones exploratorias, sin ánimo de lucro ni maliciosas (Goldstein, 2009: 510).

La curiosidad es motivo de sanción en nuestra sociedad desde que empezamos a ser conscientes de nosotros mismos y de nuestro entorno. En sus primeras etapas de vida, el ser humano es sancionado por mostrarse curioso y explorar a gatas el mundo que le rodea si no es supervisado por la autoridad (parental); en los años de juventud, la exploración implica transgredir conscientemente normas y situarse por primera vez al margen de la ley o de la moral dominante; en la etapa adulta, explorar es transgredir los límites socialmente aceptados para desarrollar una vida *estable* y, por lo tanto, es perder el derecho a la estabilidad y seguridad que ofrece el sistema; y en la vejez, explorar es, a ojos de los otros, un síntoma de infantilismo o de demencia asociado a la decrepitud. Sin embargo, la pesquisa es una virtud innata en el hacker: "Hackeamos porque somos curiosos. Difundimos lo que encontramos porque el conocimiento segregado es nuestro enemigo común" (Goldstein, 2009: 268). En este sentido, Goldstein se pregunta "cuántas más personas serán sometidas a un castigo cruel e inusual porque se atrevieron a explorar algo que entidades poderosas querían mantener en secreto" (2009: 549).

La confusión generada sobre qué es ser hacker y la criminalización de esta comunidad ha sido alentada por la autoridad. Simbólico es el discurso que el presidente Bill Clinton leyó el 22 de enero de 1999 en la National Academy of Sciences en Washington DC, titulado 'Keeping America Secure for the 21st Century'. En su perorata, Clinton identificó a los hackers como una nueva amenaza ciberterrorista para la seguridad nacional equiparable a la del terrorismo, en general, y a la del bioterrorismo, en particular.

> En la lucha por defender nuestro pueblo y valores, y avanzar siempre que sea posible, nos enfrentamos a viejas y nuevas amenazas —las fronteras libres y las revoluciones en tecnología han extendido el mensaje y los dones de la libertad, pero también han dado nuevas oportunidades a los enemigos de la libertad. Los avances científicos han abierto la posibilidad de una vida más larga y mejor. También han dado a los enemigos de la libertad nuevas oportunidades. […] los terroristas y los Estados

> fuera de la ley están ampliando los campos de batalla en el mundo, del espacio físico al ciberespacio, desde nuestras vastas masas de agua al complejo funcionamiento de nuestro propio cuerpo. Los enemigos de la paz se dan cuenta de que no nos pueden derrotar con medios militares tradicionales. Por eso están trabajando en dos nuevas formas de ataque, de las que ya habrán oído hablar: ciberataques en nuestros sistemas informáticos críticos y ataques con armas de destrucción masiva químicas, biológicas e incluso potencialmente armas nucleares. Debemos estar preparados por si nuestros enemigos intentan utilizar las computadoras para desactivar redes eléctricas, la banca, las redes de comunicación y transporte, policía, servicios de bomberos y salud, o inician acciones militares. Cada vez más, estos sistemas críticos son impulsados por y unidos entre sí con ordenadores, haciéndolos más vulnerables a la interrupción. […] ya estamos viendo la primera ola de ataques cibernéticos deliberados —hackers irrumpen en computadoras del Gobierno y de empresas, robando y destruyendo información, asaltando cuentas bancarias, haciendo cargos a tarjetas de crédito, obteniendo dinero mediante amenazas de liberar virus informáticos (Clinton, 1999)[50].

Al identificar a cualquier ciberterrorista o cibercriminal con los hackers, al incluir el ciberterrorismo como parte de la cultura hacker, Clinton —el primer presidente de la era Internet— no sólo estaba robusteciendo la ya típica estrategia de criminalización de la cultura hacker que identifica cualquier delito informático con ésta, sino que también estaba declarando formalmente la guerra a los hackers como "enemigos del Estado" (Goldstein, 2009: 261) y asentando las bases de una nueva Red de redes controlada y vigilada por el Estado-nación, bajo el pretexto de la seguridad nacional y pública. La idea de una Internet libre se mantendría sólo viva en el terreno de la utopía y de los ideales hacker.

> Retratando a aquellos de nuestra comunidad como criminales, centrándose en absurdos como los virus de correo electrónico y en crímenes «potenciales», la opinión pública puede ser fácilmente influida para que nos convierta en el enemigo, lo que hace el control más necesario a ojos de las masas (Goldstein, 2009: 589).

La idea del hacker como criminal sigue prevaleciendo en los medios de comunicación y, por lo tanto, en la conciencia colectiva, pero gracias al desarrollo de las redes sociales en línea y de medios alternativos los hackers han podido empezar a ilustrar a la sociedad sobre sus actividades, lo cual ha contribuido a que su imagen empiece a ser parcialmente reparada. Así lo ve Stallman:

> Evidentemente, hoy se dice mucho más sobre los hackers. Los medios de comunicación suelen usar el término «hacker» para significar quién rompe la seguridad informática. Pero también vemos más artículos hoy en día con una mayor tendencia que hace diez años a hablar de hackers con el significado de explorar los

[50] Traducción propia del discurso de Bill Clinton, en inglés.

límites de lo posible en cualquier campo técnico (Richard Stallman, en Quian, 2013c).

Veremos en los capítulos dedicados a WikiLeaks cómo la pelea semántica, política, ética, mediática y legal entre el Estado-nación y los hackers se ha agudizado treinta años después de sus primeras colisiones y cómo se ha ampliado el campo de batalla en el que se enfrentan hacktivistas y fuerzas del Estado-nación.

I.3. ÉTICA HACKER

> Si la naturaleza ha creado una cosa menos susceptible que todas las demás de ser poseída como propiedad excluisva, ésta es la acción del poder del pensamiento al que llamamos «idea», la cual puede ser poseída exclusivamente por un individuo en la medida en que la guarde solamente para él, pues en el mismo momento que es divulgada se pone en posesión de todo el mundo y su receptor no puede desposeerse de ella. La peculiaridad de las ideas es, también, que nadie pierde la posesión de las mismas porque las transmita por completo a otros. Aquél que recibe de mí una idea, recibe enseñanza para él sin que yo la pierda, al igual que quien enciende su vela con la mía recibe luz sin que por ello me oscurezca. Que las ideas deban difundirse libremente de un lugar a otro del planeta, para la instrucción y mejora mutua de la condición moral del ser humano, parece haber sido una pecualiaridad diseñada por la benevolencia de la naturaleza cuando las creó, como el fuego, que se propaga a todas partes sin perder su densidad en ningún punto, y como el aire en el que respiramos, nos movemos y vivimos, incapaz de ser confinado ni ser objeto de apropiación exclusiva. Por lo tanto, las invenciones no pueden ser, por naturaleza, sujetas a propiedad (Jefferson, 1813)[51].

Esta declaración del tercer presidente de Estados Unidos, y uno de los padres fundadores de esa nación, podríamos considerarla la primera declaración hacker de la historia contemporánea, pues en ella subyacen las esencias de la ética hacker.

Levy (1984: 40-46) define por primera vez la ética hacker en términos del compromiso de los hackers con la libertad de información y la meritocracia, así como su desconfianza de la autoridad y su firme creencia en que las computadoras pueden ser la base para la belleza y un mundo mejor. En concreto, Levy establece seis principios de la ética hacker:

1. El acceso a los ordenadores y a todo lo que te pueda enseñar algo sobre cómo funciona el mundo debe ser ilimitado y total.
2. Toda la información debe ser libre.
3. Hay que desconfiar de la autoridad y promover la descentralización.
4. Los hackers deberían ser juzgados por su *hacking*, sin importar sus títulos, edad, raza o posición.
5. Se puede crear arte y belleza con un ordenador.
6. Los ordenadores pueden cambiar tu vida para mejor.

[51] Traducción propia del texto original de Thomas Jefferson, en inglés.

La ética hacker refuta las tesis de Weizenbaum (1976), quien pese a reconocerles su excelencia técnica, atribuye a los hackers falta de conocimientos, de teoría y de propósitos definidos. En *The Hacker Ethic and the Spirit of the Information Age* (2001), Pekka Himanen revisa los principios definidos por Levy y enriquece su lectura, precisando que la ética hacker es heredera de la ética científica, pues las teorías se desarrollan colectivamente, los fallos son percibidos por la potencia crítica de la comunidad y los resultados y logros se publican y comparten para beneficio de la comunidad, siempre referenciando las fuentes usadas. Poner en común la información constituye un extraordinario bien para los hackers, que ven como deber de naturaleza ética compartir su competencia y pericia creando software libre y facilitando el acceso a la información y a los recursos de computación, siempre que sea posible. En concreto, el Jargon File define la ética hacker como:

> 1. La creencia de que el intercambio de información es un poderoso bien positivo, y que es un deber ético de los hackers compartir su experiencia en la escritura de código fuente abierto y facilitar el acceso a la información y a los recursos computacionales siempre que sea posible.
> 2. La creencia de que el *crackeo* de sistemas para divertirse y explorar es éticamente aceptable, siempre y cuando el *cracker* no cometa robo, vandalismo o violación de la confidencialidad.
>
> Estos dos principios éticos normativos son ampliamente, pero no de manera universal, aceptados entre los hackers. La mayoría de los hackers suscriben la ética hacker en el sentido 1, y muchos actúan en base a este escribiendo y donando software de código abierto. Algunos van más allá y afirman que *toda* la información debe ser libre y *cualquier* control de propiedad sobre ésta es malo; esta es la filosofía que hay detrás del proyecto GNU.
>
> El sentido 2 es más controvertido: algunas personas consideran que el acto de *crackeo* es en sí mismo poco ético, como un allanamiento de morada. Pero la creencia de que el *cracking* «ético» excluye la destrucción modera al menos el comportamiento de las personas que se ven a sí mismas como *crackers* «benignos» […]. Desde este punto de vista, puede ser una de las más altas formas de cortesía hacker (a) entrar en un sistema y luego (b) explicar exactamente al operador del sistema, preferiblemente por correo electrónico desde una cuenta de superusuario, cómo se ha hecho y cómo puede ser tapado el agujero, actuando como un *equipo tigre* no remunerado (y no solicitado).
>
> La manifestación más fiable de cualquiera de estas versiones de la ética hacker es que casi todos los hackers están activamente dispuestos a compartir trucos técnicos, software y (cuando sea posible) recursos informáticos con otros hackers. Redes cooperativas enormes como Usenet, FidoNet y la propia Internet pueden funcionar sin control central gracias a esto; ambas versiones se basan en y refuerzan un sentido de comunidad que puede ser el activo intangible hacker más valioso.
>
> (The on-line hacker Jargon File, version 4.4.7, 29 de diciembre de 2003).

Las aportaciones más sustanciales sobre la ética hacker en el contexto de la sociedad red vienen de la mano de Himanen (2001), quien define tres planos significativos: la ética del trabajo, la ética del dinero y la ética de las redes o nética.

La ética hacker del trabajo es una nueva moral que desafía a la ética protestante del trabajo que ha *esclavizado* a las clases trabajadoras, tal como la expuso Max Weber en su obra clásica *La ética protestante y el espíritu del capitalismo*. Frente a la laboriosidad diligente, la aceptación del deber y la rutina, el valor del dinero y la preocupación por la cuenta de resultados, Himanen (2001: 3-40) pondera el valor de la creatividad hacker, fruto de la combinación de pasión, entusiasmo, alegría y libertad que ensalza esta nueva ética del trabajo, en la que el dinero deja de ser un incentivo, un valor en sí mismo, y el beneficio se cifra en metas como el valor social que genera la labor emprendida, su transparencia y el libre acceso a la obra creada.

Junto a la ética del trabajo, el segundo plano importante de tal desafío es precisamente la ética del dinero (2001: 43-81). Aunque Himanen reconoce que la comunidad hacker no ha llegado a un consenso sobre una reformulación de la ética del dinero, asume que el hecho mismo de haberse abierto un debate en el mismo núcleo duro de la economía de la información constituye un desafío por sí radical a los imperativos de la ética protestante que reducen el valor del trabajo a una estimación exclusivamente monetaria. El hecho de proponer el libre acceso a la información, de ponerla en común, cuestiona el modelo dominante de la propiedad privativa de la información y de su monetización. La ética hacker subvierte el sistema dominante de producción, motivado exclusivamente por el dinero, al priorizar el deseo de crear algo valioso para la comunidad por encima del afán del beneficio económico. Sin embargo, Himanen advierte que no debemos ver en esta actitud ni un utopismo edénico ni una especie de aversión esencial hacia él, sino un intento de resolver qué lugar se debe asignar al dinero como motivación y qué aspectos de su influencia sobre otras motivaciones hay que evitar.

El tercer elemento sustancial presente en la ética hacker es su nética, la cual aborda ideas como la libertad de expresión en la Red y el acceso universal a ésta, que apuntan al centro de los desafíos éticos del informacionalismo (2001: 85-135). La nética alude a la relación que el hacker mantiene con las redes de nuestra actual sociedad red, incluida Internet. Tal relación se remonta al origen de la ética hacker en

la década de 1960, aunque el desarrollo de las redes ciberespaciales ha impulsado una formulación más precisa de la nética. Himanen considera un momento esencial en esta formulación el nacimiento en 1990 de la Electronic Frontier Foundation en San Francisco, creada por un grupo de filántropos libertarios con la finalidad de potenciar los derechos de libre expresión y de acceso a la información en el ciberespacio.

Para Himanen, capitalismo, comunismo y la nueva economía informacional no han hecho más que pregonar y afianzar la ética protestante, que encuentra en el monasterio medieval su precedente, mientras que la ética hacker del trabajo lo hace en la Academia, con sus sistemas de redes articuladas para compartir los hallazgos con la comunidad, sin autoridad central reguladora. Sin embargo, pese al evidente dominio que aún ejerce la ética protesante del trabajo, considera que un nuevo modelo de sociedad está emergiendo basado en los valores de la ética hacker. En su disección axiológica, Himanen (2001: 139-142) contrapone siete valores fundamentales de la ética hacker a otros tantos valores dominantes de la sociedad red y la ética protestante:

Cuadro 4: Los siete principios de la ética protestante y de la ética hacker según Himanen.

Valores de la ética protestante	Valores de la ética hacker
Dinero	Pasión
Trabajo	Libertad
Optimización	Valor social
Flexibilidad	Accesibilidad
Estabilidad	Actividad
Determinación	Preocupación responsable
Cuenta de resultados	Creatividad

Fuente: elaboración propia con las propuestas de Himanen (2001).

El primer valor que orienta la vida del hacker es la pasión, es decir, una búsqueda permanente de soluciones a problemas que le llena de energía y cuya realización le colma de gozo. A la pasión se une la libertad con la que el hacker autoorganiza sus tareas creativas y sus otras pasiones vitales, dejando siempre espacio

para el juego. Pasión y libertad son los dos valores primarios de la ética hacker y son los que han ejercido una infuencia más amplia en la comunidad hacker.

La libertad hacker supone una reapropiación del tiempo de la vida, lo cual también nos lleva a una redefinición de la ética del dinero. No en vano, en la ética protestante el dinero está intrínsecamente ligado a la expropiación del tiempo del individuo. Desde el capitalismo industrial, el tiempo es dinero para el capital y un *bien* escaso para el trabajador. Al reapropiarse el tiempo, el hacker también se reapropia su vida para vivirla de forma plena.

En esa libertad surge una voluntad que se antepone al deseo del dinero que domina a las sociedades capitalistas: la voluntad de crear y de compartir algo que tenga un valor social, que sea útil, accesible, probado, reconocido, reutilizado e incluso mejorado por otros en un proceso de aprendizaje colectivo. Este modelo hacker de aprendizaje abierto y de ilustración mutua se sintetiza en la idea platónica de que ninguna persona libre debe aprender nada por fuerza e imposición, y difiere por completo del espíritu monasterial que al maestro otorga el poder de la palabra y al discípulo impone silencio y atención. Así, el viejo modelo de comunicación de emisor activo a receptor pasivo que ha modelado en las sociedades modernas las estructuras del saber —la Academia—, del conocimiento —medios de comunicación— y del poder autoritario —gobiernos y corporaciones—, se ve desafiado por el modelo hacker abierto, transparente, horizontal, comunitario, participativo y en red. Este modelo cuestiona, además, la idea capitalista de propiedad, que también afecta a la información. Así, cuando un hacker aprende, también enseña y contribuye a que se genera un debate continuado, crítico y en evolución sobre los hallazgos.

> El proceso de aprendizaje característico del hacker empieza con el planteamiento de un problema interesante, sigue con la búsqueda de una solución mediante el uso de diversas fuentes, y culmina con la comunicación del resultado para su exhaustiva composición. Aprender más sobre un tema se convierte en la pasión del hacker (Himanen, 2001: 73).

Otro valor fundamental es la actitud que los hackers mantienen en relación con las redes, lo que Himanen llama nética, definida por los valores de la actividad y la preocupación responsable del hacker. En este contexto, actividad implica una completa libertad de expresión en la acción, privacidad para proteger la creación de un

estilo de vida individual y rechazo de la receptividad pasiva a favor del ejercicio activo de las propias pasiones.

Preocupación responsable, por otro lado, significa interesarse por los otros como un fin en sí mismo, con el deseo de librar a la sociedad red de la mentalidad de supervivencia que resulta de su lógica; esto incluye el objetivo de que todos participen en la red y se beneficien de ella, así como ayudar de forma directa a quienes quedan abandonados en los márgenes de la supervivencia.

Por último, la creatividad debe acompañar siempre al genuino hacker, siendo ésta la expresión del imaginativo uso de las habilidades propias que posee un individuo, de una asombrosa superación individual y de la donación al mundo de una aportación realmente nueva y valiosa.

Estos valores, juntos, configuran una lógica, aunque no todos son siempre compartidos por todos los hackers. Castells, en su análisis de los valores de la ética hacker propuestos por Himanen, focaliza su atención en el principio de libertad: "Libertad para crear, libertad para absorber los conocimientos disponibles y libertad para redistribuir dichos conocimientos en la forma y en el canal elegidos por el hacker"; un principio tan sustantivo en la cultura hacker que es en éste sobre el que descansa su proyecto más paradigmático: la Free Software Foundation. Pero Castells reconoce que la libertad para crear y cooperar no es el único valor radical en la cutura hacker, en la que "la innovación tecnológica constituye la meta suprema, y el disfrute personal de la creatividad es incluso más importante que la libertad" (Castells, 2001: 62).

Las interpretaciones de la ética hacker —como sucede con la propia palabra *hacker*— han tendido a reducirse al campo de la computación. Sin embargo, la ética hacker no debe ser entendida como una ética exclusiva del hacker informático, sino como un desafío social de carácter genérico, con implicaciones netamente políticas. Levy reconoce ese impulso político implícito en el *hacking*. Así lo arguye en el documental *We Are Legion: The Story of the Hacktivists*, de Brian Knappenberger:

> Siempre he visto en el *hacking* una esencia política. Los hackers, ya sean conscientes de ello o no, ya sea de una manera explícita o no, están haciendo una declaración sobre cómo debemos tratar la información (Knappenberger, 2012).

Por su parte, Stallman, aunque reconoce que "en el campo del *hacking* se pueden encontrar las dimensións ética, filosófica y política", prefiere hablar de gusto por un tipo de arte más que de una ética.

> Yo no hablo de ética hacker, para mí es simplemente gusto, un tipo de arte. Es un poco como la poesía. Hay quien compone poemas y disfruta de los poemas de otros al mismo tiempo que muestra orgullo de los poemas que ha compuesto. Hay una actitud que va con la práctica del *hack* igual que la que hay en la poesía (Richard Stallman, en Quian, 2013c).

Andy Müller-Maguhn, considera que "el argumento ético del hacker es, básicamente, utilizar la información pública y proteger la información o los datos privados" (Assange *et al*., 2012: 143). En esta lectura de la ética hacker se haya la raíz política del *hacking* y del hacktivismo, ampliamente desarrollada en 1989 en la Intercontinental Conference on Alternative Use of Technology Amsterdam (lev), ligada a la Galactic Hacker Party celebrada en la capital holandesa. En aquella conferencia se aprobó una declaración que asentó formalmente algunos de los principios políticos y libertarios hackers, basados en valores de la ética hacker como la libertad de acceso y uso de la tecnología, la libre información y la participación popular democrática efectiva. El manifiesto contempla once puntos:

- El flujo libre y sin trabas de la información es una parte esencial de nuestras libertades fundamentales y debe ser mantenido en todas las circunstancias. La tecnología de la información debe estar abierta a todos y ninguna consideración política, económica o técnica debe permitir impedir este derecho.
- El Gobierno debe ser totalmente accesible a todas las personas en cualquier momento. La tecnología de la información debe ampliar el alcance de este derecho, y no reducirlo.
- La información pertenece al pueblo y está hecha por el pueblo. Científicos y desarrolladores informáticos están al servicio del pueblo y no se les permitirá convertirse en una casta de privilegiados tecnócratas e irresponsables.
- El derecho a la información va de la mano del derecho a elegir el portador de esa información. Ningún modelo o formato de información se le impondrá a cualquier individuo, comunidad o nación. Especialmente debe ser resistida la presión para adoptar tecnología «avanzada» inapropiada. En su lugar, deben ser desarrollados métodos y equipos de fácil uso, de bajo coste y baja demanda.
- La protección de las libertades individuales son nuestra principal preocupación; exigimos que ninguna información que no sea privada pueda ser almacenada y recuperada por medios electrónicos. «Usa libremente datos públicos, protege férreamente los datos privados» es nuestro lema.

- Una vez que la información privada esté excluída de las redes informáticas, todos los datos contenidos y todas las redes deberán ser de libre acceso. La represión y la persecución del *hacking* carecerá de sentido. Mientras tanto, exigimos que cualquier ley vigente o en preparación dirigida contra individuos que hackean sin fines criminales comerciales sea retirada de inmediato.
- La tecnología informática no deberá ser utilizada por gobiernos y entidades corporativas para controlar y oprimir al pueblo; por el contrario deberá ser utilizada como un instrumento de emancipación, progreso, aprendizaje y ocio. Del mismo modo, la tecnología informática, y la ciencia en general, deberán ser retiradas de las manos de las instituciones militares.
- Toda información es también deformación. El derecho a la información está conectado inseparablemente al derecho a la deformación, el cual pertenece al pueblo. Cuanta más información se produce, más caos informativo se crea y más ruido surge. La destrucción de la información es, al igual que la producción de la información, un derecho inalienable del pueblo.
- Las computadoras y la tecnología de la información se convertirán en una herramienta para la evolución en nuestro planeta vivo. La creación de la Comunicación Artificial Inteligente salvaguardará a la Naturaleza del mal de la superpoblación comercial humana.
- Todos los canales regulares y convencionales de información deberán ser subvertidos por medio del giro y desplazamiento de la realidad fáctica meta-realística con el fin de producir caos, residuos y ruido, que a su vez se consideran portadores de información.
- La libertad de prensa se aplica por completo a las publicaciones tecno-anarquistas que aparecen de vez en cuando para liberar al pueblo de la tiranía del hombre, la máquina y el sistema.

  (Intercontinental Conference on Alternative Use of Technology Amsterdam, 1989)[52].

Podemos, finalmente, concluir que la ética hacker defiende principios básicos para un nuevo modelo social como son, entre otros, la apología de la creatividad y de la libertad del individuo, la desconfianza hacia la autoridad, la promoción de la descentralización, el libre flujo de información, la defensa de la libre expresión y del aceso universal a la información, el servicio a la comunidad y la transparencia. De esta manera, la ética hacker y el desarrollo de comunidades organizadas sobre principios hackers cuestionan la estructura social dominante en la sociedad red y propone un nuevo espíritu del informacionalismo.

[52] Traducción propia del manifiesto original, en inglés.

I.4. EVOLUCIÓN HISTÓRICA DE LA CULTURA HACKER

I.4.1. Introducción

Contar la historia de los hackers es narrar la propia historia del desarrollo de la computación, la evolución y democratización de las tecnologías digitales de la información y la comunicación, y la irrupción de la Red y de las primeras comunidades virtuales. Sus proezas son los pilares de la sociedad red.

A los criminalizados hackers debemos innumerables hitos tecnológicos de "incalculable valor para la sociedad" (Turkle, [1984] 2005: 1989): el desarrollo de lenguajes de programación, de sistemas operativos para nuestros dispositivos tecnológicos, Internet y prácticamente todo cuanto nos conecta con el mundo a través de una pantalla, un hardware y un software, pues fueron los hackers quienes contribuyeron de manera decisiva a que la alta tecnología digital se popularizase. La propia comunidad hacker presume de ello: "Los hackers construyeron Internet. Los hackers hicieron del sistema operativo Unix lo que es en la actualidad. Los hackers hacen que funcione la World Wide Web" (Raymond, 2001).

Por todo ello es necesario repasar los principales hitos hackers y el desarrollo de las distintas generaciones aparecidas durante el último medio siglo, trazando su proceso evolutivo hasta llegar a la séptima generación hacker, los hacktivistas, lo cual nos permitirá comprender sus herencias recibidas y contextualizar sus principios y acciones en la cultura hacker.

I.4.2. Génesis y taxonomía hacker

Los análisis más tempranos de Steven Levy (1984) influyeron decisivamente en la identificación de las tres primeras comunidades o generaciones hackers, que se entrecruzan y superponen entre sí (Jordan y Taylor, 2004: 10), desde sus orígenes, a finales de la década de 1950, hasta principios de los años ochenta.

1. Los hackers originales: los aficionados pioneros de la computación que experimentaron con las capacidades de los grandes ordenadores centrales de universidades de Estados Unidos como el MIT, durante las décadas de 1950 y 1960.

2. Los hackers de hardware: informáticos innovadores que a partir de la década de 1970 jugaron un papel clave en la revolución de la informática personal, posibilitando la descentralización y popularización del hardware computacional.
3. Los hackers de software: informáticos innovadores que se centraron en el desarrollo de programas informáticos cada vez más sofisticados para hardware, principalmente para ser implementado en los sistemas computacionales desarrollados por otros hackers.

Dado que el trabajo taxonómico de Levy es muy temprano, Jordan y Taylor (2004: 11-12) lo completan adicionando cuatro categorías más que se corresponden con cambios sustanciales en el *underground* informático. Estas nuevas categorías, que continúan la exploración de Levy, son:

4. Hackers/*crackers*: desde mediados de la década de 1980, estos dos términos se utilizan para describir a una persona que ilícitamente se introduce en sistemas informáticos ajenos. Sin embargo, la comunidad hacker se ha afanado en distinguirse de los *crackers*, a los que consideran otra categoría de expertos informáticos que, a diferencia de los hackers, buscan causar daños y conseguir un beneficio para ellos. Aunque Jordan y Taylor parecen contribuir con esta dualidad a fomentar la confusión conceptual sobre hackers y *crackers*, aclaran que el término *hacker*, en este sentido peyorativo, tiende a ser utilizado por individuos ajenos a la comunidad informática *underground*, especialmente en los medios de comunicación de masas, mientras que el término *cracker* tiende a ser utilizado por grupos de base tecnológica expertos en seguridad informática —tanto del *underground* como de la corriente comercial—, en un intento de salvar el término *hacker* para su más noble lectura, aplicado a individuos que manipulan ingeniosamente cualquier tecnología.
5. Microsiervos: desde mediados de la década de 1970, y más acusadamente a apartir de los años ochenta, con la explosión del mercado informático, cada vez más hackers renunciaron a su ética seducidos por el poder colonizador de la gran industria computacional, siendo Microsoft el paradigma imperial

del capitalismo tecnológico y Silicon Valley, su centro de operaciones. El neologismo inglés *microserfs* fue popularizado por el escritor y artista canadiense Douglas Coupland primero con la publicación de su relato 'Microserfs' en la revista *Wired*, el 1 de enero de 1994, y luego, en su novela de igual título, publicada en 1995, donde describe a una burguesía electrónica, una elite tecnológica al servicio de Microsoft. Su uso crítico se ha extrapolado para referirse a los hackers que se han convertido en trabajadores dúctiles y sometidos a la lógica *taylorista-fordista* en las grandes empresas tecnológicas. Aunque Bill Gates era un hacker cuando fundó Microsoft en 1975 junto con su amigo Paul Allen, su compañía se convirtió en "el enemigo público número uno" de los hackers informáticos cuando la motivación del beneficio económico se impuso a la pasión y se convirtió en el fin superior, haciendo de Microsoft el tótem para los hackers rendidos al capitalismo (Himanen, 2001: 56-57).

6. El movimiento de código abierto: el aforismo más repetido en la cultura hacker es que la información debe ser libre. Es, por así decirlo, la norma de normas de la ética hacker, que ha llevado a los más comprometidos con este principio a desarrollar software cuyo código es accesible por cualquiera que desee leerlo, interpretarlo, usarlo y modificarlo para desarrollar mejoras y software más sofisticado. Los desarrolladores de software libre y los microsiervos que crean software comercial son antagonistas. Para los primeros, todo código de programación es fuente de conocimiento y, por lo tanto, debe ser abierto para garantizar el derecho a saber de todo el mundo y fomentar el bien común; la cadena de desarrollo es libre y las modificaciones y novedades se someten a un sistema de revisión comunitaria, similar a la revisión por pares académica, para ser evaluadas y validadas, siendo valoradas principalmente la originalidad y la sofisticación. Sin embargo, para los segundos —los microsiervos— el código es fuente de ingresos económicos y, por lo tanto, debe ser privativo y secreto, para que nadie más que ellos y las empresas a las que sirven obtengan beneficios con la comercialización de software hermético que se produce industrialmente en una cadena de montaje en la que el programador es un simple operario más de una estructura organizacional centralizada y jerarquizada. La

aparición de Linux como antagonista del sistema operativo Windows de Microsoft marca la aparición de esta comunidad hacker como un actor importante en el desarrollo de la computación (Moody, 2001).

7. Hacktivistas: aunque en la década de 1980 ya emergieron grupos protohacktivistas, fue a mediados de los años noventa cuando la fusión del *hacking* con una postura política abierta articuló un nuevo movimiento social, reactivo en algunos casos, proactivo en otros. En el hacktivismo, la política proporciona la razón de ser de la actividad hacker.

Estas siete categorías recorren seis décadas de historia hacker, sobre la cual aún hoy no ha habido un consenso científico ni social que ofrezca un marco teórico y conceptual coherente y sólido al investigador para el estudio de esta cultura desde perspectivas historiográficas, tecnológicas, sociológicas, políticas, jurídicas, filosóficas, informacionales o incluso desde una necesaria transversalidad.

La criminalización de la cultura hacker y su abordaje dualista sesgado han marcado —podemos decir que incluso constreñido— su estudio e interpretación. Un claro ejemplo de esto son las cuantiosas fallas históricas y conceptuales que encontramos en las aproximaciones a los orígenes de la cultura hacker, que condicionan de manera decisiva el enfoque científico, el discurso mediático y la interpretación social del *hacking*. En particular, nos llama la atención cómo una importante parte de la literatura científica, ensayística y periodística ha pasado de puntillas sobre el *phone-phreaking* —o simplemente lo ha ignorado— en el estudio de la cultura hacker. Deducimos que esto se puede deber al enfoque reduccionista que describe el *hacking* como actividad exclusivamente computacional, a una negligencia epistemológica y/o a un virus negacionista inoculado para impugnar los orígenes hacker de emblemas del capitalismo tecnológico como Apple —cuyas raíces se hunden precisamente en la práctica del *phone-phreaking*— y, en general, de toda nuestra base tecnológica contemporánea, para evadir así lo que parece una verdad incómoda o, en el argot posmodernista, políticamente incorrecta.

I.4.3. *Phreaks* y primeros hackers computacionales

Fue a partir de la década de 1980 cuando los hackers se dieron a conocer al mundo. Pero la historia de la comunidad hacker comienza mucho antes, en el ocaso de la década de los años 1950 y principios de la de 1960. Para que la intrincada cultura hacker cristalizase tuvo que haber un caldo de cultivo previo. Y este se encuentra en la emergencia de dos corrientes confluyentes que nacieron a la par: los *phone phreaks* y los primeros hackers computacionales.

Los neologismos *phreak* y *phreaking* fueron acuñados para describir la actividad hacker vinculada al estudio, exploración y experimentación de sistemas de telecomunicaciones, principalmente de los equipos y sistemas de las redes telefónicas. El término es un juego lingüístico que fusiona las palabras inglesas *freak* y *phone*. Su uso para describir a personas que utilizan diversos dispositivos electrónicos o trucos para introducirse en las redes telefónicas, para explorar y manipular el sistema y/u obtener llamadas gratuitas (Jordan y Taylor, 2004: 14), se empezó a popularizar a finales de la década de 1950 y alcanzó su cenit en la segunda mitad de los años sesenta y primera mitad de los setenta.

> La red telefónica fue el sistema arquetípico de los primeros precursores de los hackers, los *phone-phreaks*; luego, Internet aportó el siguiente sistema técnico complejo listo para la exploración (Jordan y Taylor, 2004: 122).

Aunque en su escueta aproximación al *phreaking* Jordan y Taylor categorizan a los *phreaks* como una suerte de protohackers, estos deben ser incluidos en la categoría de hackers originales de Levy. No en vano, los hackers de teléfonos jugaron un papel decisivo en la configuración de esta cultura, hasta tal punto, que la revista hacker *2600* o el mismísimo Steve Wozniak —cofundador de Apple— se reconocen deudores de los hallazgos e hitos tecnológicos de los *phreaks* (Goldstein, 2009; Wozniak, 2014).

Meyer y Thomas ofrecen una descripción más detallada y extensa, aunque cometen también el error de despojar a los *phreaks* de sus esencias hackers. Su justificación es tan simplista como reduccionista, limitando el *hacking* única y exclusivamente a la computación:

> Aunque *phreaking* y *hacking* requieren habilidades distintas, *phreaks* y hackers tienden a ser asociados en el mismo tablero. A diferencia de los hackers, que intentan dominar un sistema informático y su estructura de mando y seguridad, los

> *phreaks* se esfuerzan por dominar la tecnología de las telecomunicaciones (Meyer y Thomas, 1990: 25).

En todo caso, estos dos autores coinciden con Sterling (1992) en liberar a los *phreaks* —al menos a los genuinos, aquéllos que merecen tal distinción— del estigma criminal que, como en el caso de los hackers computacionales auténticos, han sufrido los exploradores de los sistemas telefónicos, para quienes el fraude o las estafas son anatema, como para los hackers informáticos lo son la destrucción de cualquier sistema ajeno o el robo de datos privados. Su objetivo —concluyen tanto Meyer y Thomas como Sterling— es explorar y aprender lo máximo posible sobre los sistemas telefónicos y las redes de telecomunicaciones, y compartir el conocimiento adquirido. Pero para acceder al conocimiento, los *phreaks*, como sus colegas informáticos, tienen que recurrir a métodos legalmente cuestionables, a veces manifiestamente ilegales. Meyer y Thomas describen tres características fundamentales del *phreaking* que lo sitúan bajo el paraguas de la ética hacker, sin que estos dos autores asuman tal proposición: la búsqueda de conocimiento, un propósito ideológico de oposición a los potenciales peligros del control tecnológico y el disfrute de asumir riesgos (Meyer y Thomas, 1990: 30).

Sterling también intenta aportar un poco de luz en los más tempranos análisis del *phreaking*, acercándolo más a la cultura hacker:

> Debido a que la red de telefonía es anterior a la red informática, los infractores conocidos como «*phreakers*» son anteriores a los infractores conocidos como «hackers». En la práctica, hoy en día la línea que separa el «*phreaking*» y el «*hacking*» está muy difuminada, de igual modo que la que separa teléfonos y computadoras. El sistema telefónico ha sido digitalizado, y las computadoras han aprendido a «hablar» a través de líneas telefónicas (Sterling, 1992).

En ambas corrientes, Sterling identifica un goce en la ejecución de la acción intrusa, y aunque reconoce que las distinciones entre hackers (informáticos) y *phreaks* "prácticamente han desaparecido", considera que los primeros "están muy interesados en el «sistema» en sí mismo y disfrutan relacionándose con las máquinas", mientras que los segundos "son más sociales, manipulando el sistema de una manera primitiva pero funcional para comunicarse con otros seres humanos de una manera rápida,

barata y subrepticia" (Sterling, 1992). Pero en su distinción, mantiene a los *phreaks* fuera de la categoría hacker, obviando la elasticidad experimental del *hacking*, que reduce al campo de la computación.

Fue precisamente un habilidoso programador experto en seguridad informática y *phreak* el primero en convertirse en mito viviente en la comunidad hacker: John Thomas Draper. El *hack* por el que pasó a ser idolatrado en el *underground* tecnológico se originó en un descubrimiento fortuito que podría haber sido considerado trivial, incluso estúpido, de no ser por el ingenio de Draper y sus ulteriores secuelas en la cultura hacker. El hallazgo, un simple silbato promocional de plástico en una caja de cereales, se convirtió en el objeto *mágico* que revolucionó e impulsó el movimiento hacker de una manera decisiva. Y tal vez sea éste el más ilustrativo ejemplo de la pulsión creativa hacker.

A comienzos de la década de 1970, Draper descubrió —gracias a unos amigos *phreaks* invidentes que habían estado experimentando con sus habilidades sensitivas— que modificando levemente el silbato que contenían las cajas de cereales Cap'n Crunch, comercializadas por la empresa Quaker Oaks, se podía conseguir el mismo tono que el pitido previo de las llamadas telefónicas de larga distancia, de 2.600 herzios. Al soplar el silbato en el teléfono en el momento oportuno, se engañaba al sistema de conmutación de AT&T y se conseguía acceso para hacer una llamada de larga distancia sin coste.

Fue así como a John Thomas Draper —conocido desde entonces como Captain Crunch— se le ocurrió crear un dispositivo, con teclado numérico, que generase el resto de tonos que utilizaban las centralitas telefónicas. La noticia corrió de boca en boca, las cajas azules se multiplicaron y el fenómeno acabó en la revista *Esquire*, en su edición de octubre de 1971, en un artículo firmado por Ron Rosenbaum titulado 'Secrets of the Little Blue Box'. Muy pronto, un estudiante de la University of California, en Berkeley, llamado Steve Wozniak, que había pedido consejos a Draper atraído por aquel artículo de Rosenbaum, empezó a crear sus propias cajas azules —la primeras digitales— y a venderlas junto con su amigo Steve Jobs por 150 dólares cada aparato. Entre sus hazañas se recuerda aún una llamada gratis que Wozniak hizo al Vaticano, haciéndose pasar por Henry Kissinger, en la que solicitaba hablar con el Papa; al otro lado del teléfono le contestaron que eran las cinco de la mañana y que el

pontífice estaba durmiendo (Isaacson, 2011). En 1976 — sólo un año después de que otro hacker llamado Bill Gates fundase Microsoft junto con su colega Paul Allen—, Wozniak y Jobs crearon Apple, empresa que no habría existido si no hubiesran conocido las *blue boxes* y a Drapen (Barlow, 1990; Wozniak, 2014). Durante una estancia en la cárcel, tras ser arrestado en 1977 por sus *hacks*, Drapen también creó el procesador de texto Easy Writer para la serie de computadoras Apple II, lanzada en 1979; dos años más tarde desarrolló una versión renovada para el primer PC de la empresa IBM.

La cultura hacker parió dos de los mayores negocios y emblemas del capitalismo tecnológico —Apple y Microsoft— y fue decisiva en el desarrollo de lo que Levy llamó en 1984 "la revolución computacional". Pero el capitalismo aparcó las utopías e ideales de muchos de aquellos jóvenes hackers, que encontraron en el software y el hardware privativos un negocio multimillonario del que vivir.

> Todavía no estamos seguros de qué le pasó a la bandera pirata que una vez voló sobre la sede de Apple Computer, pero sí sabemos que lo que antes era un fenómeno *nerd* respaldado por una creencia idealista en la libertad de información se convirtió en el poderoso afrodisíaco detrás de atractivas ofertas públicas de venta de acciones. El Che Guevara con opciones sobre acciones (Hawn 1996: 2)[53].

Ilustración 3: Bandera pirata en las oficinas de Apple, diseñada por Susan Kare en 1983.

Foto: Andy Hertzfeld. Fuente: floklore.org

El *phreaking* no sólo inspiró la fundación de una de las compañías que más ha influido en la configuración de una cultura y una economía globales mediadas por las

[53] Traducción propia del texto original, en inglés.

tecnologías digitales, también originó los primeros medios de comunicación especializados en *hacking*, que contribuyeron de manera decisiva a la configuración de la cultura hacker: primero, el boletín de noticias *YIPL/TAP*, entre 1971 y 1984, al que sucedió en el año de su defunción la revista especializada en información técnica para *phreaks* y hackers informáticos *2600: The Hacker Quartely*, que *oficializó* la confluencia del *phreaking* y del *hacking* informático.

La corriente computacional ha sido la más influyente en la cultura hacker. Como corriente dominante, ha determinado —y limitado— los enfoques sobre los estudios e interpretaciones del *hacking*. Sus orígenes están ligados estrechamente al ferrocarril, más en concreto, al mundo de las maquetas de trenes. Al igual que en otras universidades de Estados Unidos, en el Massachusetts Institute of Technology existían clubs que congregaban a alumnos del campus interesados en distintas actividades. Uno de aquellos grupos era el Tech Model Railroad Club, creado en 1946. El club giraba alrededor de maquetas de trenes y sus miembros se dedicaban a recorrer el campus para conocer a fondo sus sistemas de comunicación.

El Tech Model Railroad Club tenía dos grupos de trabajo: por un lado, aquéllos que se encargaban de construir y decorar las maquetas de trenes, y por otro, el Comité de Energía y Señales, que adoptó aquellas máquinas como su juguete tecnológico favorito y para el cual desarrollaron nuevas herramientas de programación, un nuevo argot y una nueva cultura (Raymond, 2001). Aquellos protohackers escribían sus propios programas, los testaban, los modificaban y los depuraban borrando trozos de código inútiles. A aquellas modificaciones y mejoras las denominaron *hacks* y a sus autores, hackers: "La cultura informática del MIT parece haber sido la primera en adoptar el término *hacker*" (Raymond, 2001).

Eric S. Raymond sitúa la adquisición del primer PDP-1 (Programmed Data Processor-1) en el MIT como el acontecimiento clave, el auténtico *Big Bang* de la cultura hacker. La incipiente industria de la computación estaba empezando a comercializar sus primeras máquinas y las universidades eran uno de sus principales nichos de mercado. La PDP-1 fue la primera computadora fabricada en serie por Digital Equipment Corporation (DEC). Trabajaba a una frecuencia de 200 KHz, realizaba cien mil operaciones por segundo, usaba rollos de cinta perforada (que no tarjetas) como sistema de entrada del software y, como periféricos, admitía el uso

de una máquina de escribir a modo de consola de entrada y también un monitor CRT a modo de salida. Un auténtico juguete para aquellos primeros hackers del MIT liderados por Peter Samson. No tardaron en desarrollar uno de los primeros procesadores de textos que se conocen, programas para realizar cálculos de trigonometría, un compilador de armonía para reproducir música de Bach y Mozart, canciones populares y villancicos de Navidad, o el primer videojuego para computadora de la historia, *Spacewar!*, de Steve Russell.

El Tech Model Railroad Club se convirtió en el núcleo del Laboratorio del Artificial Intelligence Laboratory del MIT, que se convirtió en el principal centro mundial de investigación en Inteligencia Artificial en la década de los años ochenta del siglo XX. "Su influencia se extendió mucho más allá de 1969, el primer año de ARPAnet" (Raymond, 2001).

Otro de los hitos informáticos protagonizado por los hackers computacionales fue el desarrollo del Incompatible Timesharing System, un innovador y revolucionario sistema operativo de tiempo compartido, en el que se comenzó a trabajar en la segunda mitad de la década de 1960 en el Laboratorio de Inteligencia Artificial del MIT, con la colaboración del Proyecto MAC (Project on Mathematics and Computation) de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), del Gobierno estadounidense, auspiciadora de la red de ordenadores ARPAnet. El Incompatible Timesharing System fue resultado de la pasión hacker (Turkle, [1984] 2005: 189). Su nombre fue un *hack* del anterior sistema operativo de tiempo compartido del MIT, el Compatible Time-Sharing System, presentado en 1961.

El Incompatible Timesharing System se desarrolló como la respuesta hacker al sistema de seguridad incorporado al proyecto Multics (Multiplexed Information and Computing Service), sistema operativo de tiempo compartido puesto en marcha en 1964 por el MIT en colaboración con General Electric y los laboratorios Bell. Posteriormente, en 1969, Multics tuvo su propio *hack*, el archiconocido Unix, originalmente Unics (UNIplexed Information and Computing Service), sistema operativo portable, multitarea y multiusuario desarrollado por un grupo de empleados de los laboratios Bell que habían abandonado el proyecto original. En 1971, Richard Stallman, considerado el hacker más famoso de todos los tiempos, ingresó en el MIT y empezó a colaborar en el proyecto Incompatible Timesharing System para mejorar el

sistema. Años después, en 1983, a punto de oficializarse la existencia de la cultura hacker, Stallman presentó un nuevo sistema revolucionario, compatible con Unix, que dio un nuevo impulso a la comunidad hacker —parte de la cual empezaba a dejarse fagocitar por la rama comercial de la computación, abandonando el uso y desarrollo de software libre para pasarse al *lado oscuro* del software privativo— y ratificó su papel central en el desarrollo de innovaciones tecnológicas abiertas y libres. El Proyecto GNU supuso la salida de Stallman del MIT y la defunción no tanto de la cultura como de la actividad hacker en este instituto, convertido en templo de la ciencia y la tecnología.

Durante las décadas de 1960 y 1970 se asentaron los cimientos de la cultura hacker, en cuyo seno se desarrollaron grandes avances tecnológicos de los que somos herederos. Y el MIT se consagró como la catedral del hacking. Aquellos jóvenes apasionados de la computación "escribieron otros programas influyentes y pasaron a formar parte de la vida intelectual del Artificial Intelligence Laboratory del MIT" (Turkle, [1984] 2005: 189).

El término *hacker* empezó a ser adoptado como insignia por la incipiente comunidad de tecnólogos y científicos computacionales que estaba germinando en distintas universidades de Estados Unidos, pero que tuvo su principal núcleo en el Massachusetts Institute of Technology, en concreto, en el Tech Model Railroad Club y en el Artificial Intelligence Laboratory. A la par, en Stanford, Berkeley, CalTech, Carnegie Mellon y otros centros del país se fueron desarrollando otros grupos hackers de manera independiente.

Un acontecimiento crucial para las primeras comunidades hackers y, a la postre, para el mundo, fue la culminación de ARPAnet —el embrión de lo que sería Internet—, la primera red informática transcontinental de alta velocidad, a cuyo desarrollo contribuyó vigorosamente la comunidad hacker (Hannemyr, 1999). Los orígenes de ARPAnet se encuentran en el Departamento de Defensa de Estados Unidos, como experimento para las comunicaciones digitales. La idea era enlazar múltiples ordenadores remotos en red de laboratorios científicos para compartir recursos (Hafner y Lyon, 1996). Su desarrollo se extendió hasta las universidades, laboratorios de investigación y contratistas de defensa, y se permitió a investigadores de todas partes usar esta red para intercambiar información con una velocidad y

flexibilidad sin precedentes, dando un gran impulso al trabajo colaborativo y aumentando el ritmo e intensidad de los avances tecnológicos. A través de aquellas autopistas electrónicas, cientos de hackers se reunieron en una masa crítica; en lugar de trabajar en pequeños grupos aislados, se autodescubrieron como una tribu en red (Raymond, 2001). Con el desarrollo de la red electrónica de comunicaciones, los distintos campus universitarios pudieron conectarse remotamente unos con los otros y los hackers encontraron en los buzones de correo electrónico una vía rápida y eficiente (Goldstein, 2009: 148), prácticamente instantánea, para compartir experiencias, conocimientos, ideas, habilidades. Y así crearon una nueva cultura, la hacker.

En ARPAnet asentaron y propagaron las bases de esta nueva cultura con sus primeras listas del argot hacker, las primeras discusiones sobre ética hacker, la primera literatura hacker… La primera versión del Jargon File, desarrollada entre 1973 y 1975, se erigirió en el documento que dotó de un lenguaje propio y, por lo tanto, de entidad e identidad, a la comunidad hacker. Su desarrollo fue colaborativo y en red, y se convirtió en uno de los documentos definitorios de la cultura hacker, aunque no fue publicado hasta el año 1983 con el título *The Hacker's Dictionary*[54].

Fue precisamente hasta 1983 que la red militar y la académica convergieron en este proyecto común llamado ARPAnet. Pero desde 1983, ciencia y militarismo divergieron por motivos de seguridad y sus contenidos se empezaron a distribuir por dos redes distintas: el Departamento de Defensa de Estados Unidos empezó a usar la red de comunicación militar MILNET (Military Network), mientras que ARPAnet se mantuvo como red académica y científica, y dio origen más tarde a Internet. Durante un tiempo de transición, sin embargo, ambas redes estuvieron conectadas por medio de un *gateway*[55]. "Esto resultó ser muy conveniente para los hackers, ya que ahora sabían dónde estaban todos los equipos militares" (Goldstein, 2009: 145).

ARPAnet fue decisiva para la configuración de la cultura hacker. El posterior desarrollo de Internet y su popularización a partir de la década de 1990 hizo de este metamedio el ecosistema paradigmático para la cooperación y el trabajo comunitario orientados, primero, a la innovación tecnológica y a la ampliación permanente,

[54] Aquella primera versión está fuera de catálogo, pero Eric S. Raymond realizó otra revisada y ampliada, titulada *New Hacker's Dictionary*, editada por *MIT Press* en 1991, 1993 y 1996.
[55] *Gateway* es una puerta de enlace o pasarela que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

compartida e ilimitada del conocimiento y, posteriormente, a la defensa activa de la información libre. "Su propia existencia [la de Internet] fue vista como una especie de triunfo para los hackers, ya que muchos de ellos participaron activamente en la construcción de algo verdaderamente sustancial que inevitablemente sería descubierto por las masas" (Goldstein, 2009: 277).

No en vano, los logros de la comunidad hacker vinculada a la computación "constituyen la nueva base tecnológica de la sociedad emergente: Internet y la Red de redes (lo que en conjunto podríamos llamar la Red), el ordenador personal, así como una parte importante del software utilizado para que todo ello funcione" (Himanen, 2001: vii). E Internet, en particular, abrió nuevos horizontes sociopolíticos:

> Mientras que su predecesor, el ARPAnet de los 60 y 70, se desarrolló bajo la autoridad de los militares, lo que ha evolucionado desde entonces es un verdadero bastión de la libertad de expresión y el empoderamiento de los individuos (Goldstein, 2009: 832).

Con el advenimiento de la informática personal y la comunicabilidad de las redes se popularizó el desarrollo y uso de los BBS (Bulletin Board System), tablones de anuncios electrónicos (Castells, 1999: 386) accesibles a cualquier persona que tuviese una computadora, un módem y un teléfono, y que se usaron para la comunicación y el intercambio de información entre hackers de todo el mundo (Goldstein, 2009: 224), contribuyendo de manera decisiva a forjar su identidad en comunidades virtuales.

> Los BBS fueron, en la década de los 80 y 90, la Internet de la gente de la calle, la red a la medida humana, precursoras de todo lo que vendría después y centros de aprendizaje para muchos programadores, administradores y, en general, hackers (Molist, 2014) .

Desde su invención, los tablones de anuncios electrónicos fueron "la sangre del *underground* digital" (Sterling, 1992). El primer BBS fue creado y lanzado por Ward Christensen y Randy Suess el 16 de febrero de 1978, en Chicago (Estados Unidos). Su sistema se llamó Computerized Bulletin Board System (CBBS), el primer tablón eletrónico público, precursor de las redes sociales en línea. Gracias a ellos, la segunda generación de hackers creó su propia infraestructura de comunicación, ante las restricciones impuestas para acceder a ARPAnet. FidoNet, PeaceNet, Usenet o The

WELL (Whole Earth 'Lectronic Link) fueron las primeras manifestaciones de una nueva estructura social basada en redes de cooperación electrónicas baratas, ubicuas, descentralizadas y desreguladas, por las que la información fluye libre y la privacidad puede ser protegida (Sterling, 1992; Jordan, 1999), y sirvieron para articular formas de protohacktivismo.

> En 1989, las protestas electrónicas contra los sucesos de Tiananmen en China, vía las redes informáticas manejadas por los estudiantes chinos del extranjero, fueron una de las manifestaciones más conocidas del potencial de los nuevos mecanismos de comunicación. Los Sistemas de Tablones de Anuncios no necesitaban redes informáticas complicadas, sólo ordenadores personales, módems y la línea telefónica. De este modo, se convirtieron en los tablones electrónicos de noticias de toda clase de intereses y afinidades, creando lo que Howard Rheingold denomina «comunidades virtuales» (Castells, 1999: 386-387).

Los hackers fueron los creadores de las primeras comunidades virtuales (o primeras redes sociales en línea). A finales de la década de 1980 también se empezó a popularizar el uso de un nuevo protocolo de comunicación, el Internet Relay Chat (IRC), que dispuso nuevos entornos basados en la comunicación electrónica en tiempo real entre usuarios, mediante mensajes de texto. Creado en 1988 por Jarkko Oikarinen, del Departamento de Ciencias de Procesos de la Información de la Universidad de Oulu, muy pronto hackers, activistas y disidentes empezaron a conectarse en diversos IRC y a descubrir el potencial político-social de las redes de chat. En 1991, usuarios de Kuwait utilizaron redes de chat para informar sobre la guerra del Golfo, y en la Unión Soviética se hizo lo propio durante el intento de golpe de Estado previo a la disolución de régimen comunista. Este sistema, que anticipó el advenimiento de las actuales redes sociales en línea, sirvió también a los hackers para crear sus propias salas de reuniones virtuales, como EfNet, UnderNet, IRCnet o DALnet (Molist, 2014).

Desde inicios del siglo XXI, la masa internauta fue migrando de los servicios de chat a las redes sociales en línea que proveen mastodontes comerciales como Facebook o Twitter, pero los hackers, y más precisamente los hacktivistas, han mantenido las redes de chat como medio de comunicación en la Red. Un buen ejemplo es el AnonOps (Anonymous Operations) IRC, plataforma transnacional de comunicación frecuentada por miembros de Anonymous y otros activistas[56].

[56] Disponible en: https://anonops.com/ (último acceso: 20 de septiembre de 2015).

Los hackers constituyeron en los subterráneos de la computación la primera cultura articulada en redes electrónicas. "El *underground* informático es a la vez un estilo de vida y una red social", aclaran Meyer y Thomas (1990: 12). Juntas, en red, las primeras comunidades virtuales configuraron, a través de circuitos electrónicos, los primeros medios sociales en línea y la primera cultura hacker, movimiento intelectual que básicamente pretendía explorar lo desconocido, documentar los arcanos y hacer lo que otros no podían. Los hackers encontraron así su medio natural, la Red de redes, que agudizó las motivaciones políticas que yacen en la cultura hacker.

> Internet nace y se construye sobre el trabajo de este nuevo tipo de investigador que, con tendencias cada vez más marcadas al activismo, reclama libertad plena de movimientos: libertad plena de acceso a la información, para la manipulación de código, para hacer públicos los resultados de su investigación y hacer uso de los resultados del trabajo de otros investigadores, etc. Resultado de una necesidad operativa básica, la comunidad hacker imprime a la red y a los primeros foros de creatividad colectiva una impronta libertaria en un sentido liberal que exige el reconocimiento pleno y radical de los derechos básicos a la libre comunicación y expresión, aplicados a conciencia y hasta sus ultimas consecuencias en el terreno de la investigación y la generación de saberes compartidos. Esta es la característica definitiva de un hacker (su concepción/relación con la información y el conocimiento), muy lejos de la caricatura delictiva y criminalizadora que se ofrece al gran publico desde los mass-media (Sádaba Rodríguez y Roig Domínguez, 2004).

I.4.4. 1984: estallido hacker contra la distopía *orwelliana*

Las primeras referencias públicas escritas sobre los hackers son tardías. La primera mención registrada de la palabra *hacker* en su sentido moderno apareció en 1976 en el libro de Joseph Weizenbaum *Computer Power & Human Reason*: "El programador compulsivo, o hacker, como se autodenomina, es por lo general un técnico soberbio".

Weizenbaum describe a los primeros hackers como personas intelectualmente brillantes, de aspecto desaliñado, capaces de trabajar con una computadora hasta la extenuación, veinte o treinta horas prácticamente seguidas, alimentados únicamente de Coca-Cola, café y sándwiches para no perder el compás.

> Su ropa arrugada, sus caras sin afeitar ni lavar, y sus pelos revueltos, todo muestra que se han evadido de sus cuerpos y del mundo en el que se mueven. Existen, al menos cuando lo consiguen, solamente a través de y para las computadoras. Son vagabundos informáticos, programadores compulsivos. Son un fenómeno internacional (Weizenbaum, 1976: 115).

Sin embargo, no fue hasta los años ochenta del siglo XX cuando la palabra *hacker* se empezó a popularizar por su uso en medios de información, tanto especializados como generalistas, y en libros dedicados a esta comunidad. Según recoge el Oxford English Dictionary, en mayo de 1983 la revista *Byte* publicó una de las primeras referencias al *hacking*, situando el origen de la palabra en los laboratorios del Massachusetts Institute of Technology:

> «Hacker» parece haberse originado en el MIT. La expresión original germano/yiddish se refería a alguien tan inepto como para hacer muebles con un hacha, pero de alguna manera el significado ha cambiado de modo que ahora generalmente se refiere a alguien obsesionado con la programación y las computadoras pero que posee un alto grado de habilidad y competencia (Oxford English Dictionary, 2000).

Por entonces, los medios empezaron a poner su foco sobre los hackers y sus destacadas y llamativas actividades. Ese mismo año, el 3 de octubre de 1983, el periódico británico *Daily Telegraph* se hacía eco de una penetración hacker en el sistema de mensajería confidencial de British Telecom cuando se hacía una demostración en directo en la BBC. Su definición de *hacker* fue la siguiente: "[...] en la jerga de las computadoras, fisgón electrónico que burla los sistemas informáticos de seguridad". Lo cierto es que el término *hacker* empezaba a popularizarse por aquel entonces en Estados Unidos, donde la comunidad hacker ya gozaba de una dilatada tradición de dos décadas, pero también en Europa. La fundación en 1981 del Chaos Computer Club de Berlín –la mayor asociación de hackers de Europa– supuso un hito en el Viejo Continente. Pero el mundo se preparaba para un año clave para su reconfiguración: 1984 no sólo estaba marcado en rojo como el año del Gran Hermano de George Orwell, también sería el año en el que se empezaron a fortificar los pilares de una nueva cultura destinada a derrumbar el sistema de vigilancia y control institucionalizado y a liberar la información y el conocimiento.

En 1984 se produjeron una serie de acontecimientos claves en la historia de la cultura hacker, de la computación y del activismo, estrechamente relacionados entre sí bajo el dominio simbólico de la novela de George Orwell: el lanzamiento al mercado del primer Macintosh de Apple; la publicación del libro *Hackers: Heroes of the Computer Revolution*, de Steven Levy; las apariciones de las revistas hackers *2600: The Hacker Quarterly*, en Estados Unidos, y *Datenschleuder*, en Alemania; el inicio

del proyecto GNU y de la Free Software Foundation, liderados por Richard Stallman; la celebración de la primera Hackers' Conference estadounidense, en San Francisco, y la del primer Chaos Communication Congress, en Hamburgo (Alemania); la publicación del libro de ciencia ficción y obra fundacional del *cyberpunk* *Neuromancer*, de William Gibson; la firma del Acuerdo Valletri por varias organizaciones internacionales no gubernamentales, para iniciar nuevos métodos de colaboración en red mediada por computadoras; la creación del ya mítico grupo hacker Legion of Doom, con miembros repartidos por todos los Estados Unidos, y la aparición de la que es reconocida como primera organización hacktivista en el mundo, Cult of the Dead Cow, creada en Lubbock (Texas).

El 22 de enero de 1984, dos días antes de que Apple lanzase al mercado su primer Macintosh, millones de telespectadores estadounidenses fueron impactados durante la celebración de la Super Bowl —el mayor acontecimiento deportivo de aquel país— por un anuncio de la marca de la manzana mordida dirigido por el célebre director de cine Ridley Scott. No fue casualidad que Apple aguardase a que comenzara el año con el que Orwell tituló su sombría novela para iniciar la campaña publicitaria de su nuevo producto. IBM había sido tradicionalmente considerado antagonista de la cultura hacker por quienes profesaban el *hacking* y Steve Jobs, ideólogo de Apple, se había curtido en la cultura hacker en sus primeros años, antes de pasarse al *lado oscuro* y traicionar los ideales hackers. Aquel anuncio aún hoy se considera uno de los mejores anuncios televisivos de la historia y permanece en la memoria colectiva de millones de personas. Los Macintosh venían para liberar al mundo de IBM, identificado por Jobs y los suyos como el auténtico Gran Hermano. En pleno fulgor hacker y efervescencia tecnológica, pocos podían imaginar que tres décadas después Apple y Steve Jobs serían vistos por los hackers como dignos herederos de IBM, como el Gran Hermano del siglo XXI.

Veinticinco años después del estreno de este anuncio publicitario, Jon Lech Johansen —hacker noruego conocido por el alias DVD Jon, desarrollador del famoso programa DeCSS (Decoder Content Scramblins System)[57]—, realizó un *remake* de aquel anuncio en el que ahora es Apple quien representa al Partido, a la dictadura, y Steve Jobs, el Gran Hermano. Aunque no hay referencias explícitas a la marca ni a su

[57] Ir a página 162.

fundador, el parecido del personaje de la pantalla —el gran dictador— con Steve Jobs es más que razonable, mientras la masa —seres anodinos— se muestra alienada por un aparato electrónico que simula ser un iPod, el producto con el que Apple inició una nueva era tecnológica. Jon Lech Johansen hizo este montaje para anunciar una nueva versión de la aplicación DoubleTwist que, entre otras cosas, sirve como puente entre iTunes y dispositivos que no son de Apple (un *hack* para saltar las barreras que Apple impone a sus consumidores con su sistema cerrado).

Ilustración 4: Imagen del anuncio del lanzamiento de DoubleTwist.

Fuente: captura de pantalla propia tomada de https://youtu.be/tdVzboF2E2Q (último acceso: 12 de mayo de 2014).

Nada parece fruto de la casualidad en la cultura hacker. En el año del Gran Hermano, Emmanuel Goldstein —enigmático personaje clave en la novela de Orwell, enemigo público número uno del Partido y amenaza del Estado totalitario y de su sistema de control y vigilancia— se encarnó en el editor de la nueva revista *2600: The Hacker Quaterly*. Esta publicación de culto entre la comunidad hacker no sólo se convirtió en referencia contracultural, en mito del *underground* computacional, sino también en un ariete de lo que sería el hacktivismo. El sobrenombre fue tomado por el hacker y hacktivista Eric Gordon Corley para fundar en enero de 1984 esta revista, editada por su organización no lucrativa 2600 Enterprises, Inc.

1984 fue también el de la *presentación oficial* de los hackers en sociedad, con la primera y gran apología de la cultura hacker, obra fundacional, fundamental y de culto: *Hackers: Heroes of the Computer Revolution*, de Steven Levy, elevó por primera vez a los hackers a categoría de clase social, y más concretamente, de elite en

la vanguardia cultural y tecnológica. En respuesta a este libro, Stewart Brand y sus socios del Whole Earth y The Point Fundation organizaron la primera Hackers' Conference en Estados Unidos. La reunión tuvo lugar en San Francisco y a ella acudió buena parte de la elite hacker, incluidos Steve Wozniak, Ted Nelson, Richard Stallman, John Draper, Richard Greenblatt, Robert Woodhead, Bob Wallace y Burrell Smith, este último, uno de los padres del ordenador Macintosh de Apple.

> Los hackers de la Hackers' Conference tenían poco o nada que ver con los del *underground* digital. Al contrario que éstos, los hackers de esta conferencia eran en su mayoría expertos ejecutivos californianos de la alta tecnología, consultores, periodistas y empresarios. (Este grupo era el tipo exacto de «hackers» que más fácilmente reaccionarían con furia militante ante cualquier degradación criminal del término «hacker»). (Sterling, 1992).

En aquel encuentro, Burrell Smith —el hacker que diseñó la placa madre del primer prototipo del Macintosh de Apple— dijo:

> Se puede hacer casi de todo y ser un hacker. Se puede ser un carpintero hacker. No es preciso disponer de alta tecnología, pienso que tiene que ver con la artesanía y con el hecho de dar importancia a lo que uno hace (Himanen, 2001: 7).

Pero lo más sustancial de aquel encuentro fue el adagio que Stewart Brand convirtió en el faro hacker: "La información quiere ser libre" (Brand, 1987: 202). El mensaje no dista del de Thomas Jefferson (1813) cuando éste dice que "las ideas deberían difundirse libremente". El profesor Roger Clarke (1999) —miembro de la Australian Computer Society y la Association for Information Systems— reconoce un atecedente más reciente en el Tech Model Railroad Club del MIT, la cuna del *hacking*, donde se decía: "La información debe ser libre". Este aforismo fue pronunciado por el científico computacional del MIT Peter Samson en el año 1959, según esclarece Edwin Parsons a Clarke en un correo electrónico enviado el 13 de agosto de 1999 al boletín Tasty Bits from the Technology Front[58].

Al otro lado del Atlántico, los hackers europeos celebraron también en 1984, en Hamburgo, la primera edición del Chaos Communication Congress, organizado por

[58] Tasty Bits from the Technology Front fue un boletín electrónico de noticias pionero y gratuito dirigido a personas interesadas en tecnologías de la comunicación y comercio en Internet. El servicio era prestado por Technology Front, una consultora especializada en negocios y marketing en Internet. Estuvo operativo desde finales de 1994 hasta mediados del año 2000. Su sitio web aún es accesible en Internet: http://tbtf.com/ (último acceso: 25 de septiembre de 2014).

el Chaos Computer Club, el colectivo hacker más antiguo y respetado del Viejo Continente. Estos hackers alemanes también lanzaron ese mismo la revista *Datenschleuder*, creada por Wau Holland, cofundador del Chaos Computer Club.

A la par, William Gibson publicó en 1984 la obra fundacional del *cyberpunk* y del ciberespacio[59], *Neuromancer*, una novela de ciencia ficción en la que por primera vez se habló del espacio cíber y de la que bebieron los *cypherpunks* (criptopunnks) en la década de 1990, en su confrontación contra el secreto y en su defensa activa del derecho a la privacidad en la Red. La obra de Gibson inspiró también la saga fílmica *cyberpunk* de culto *Matrix*.

1984 fue también el año en que Richard Stallman, considerado el gran gurú hacker, abandonó el Massachusetts Institute of Technology para centrarse en el proyecto GNU y así,

> cristalizar en la Free Software Fundation el núcleo iniciático de un movimiento colectivo y social que introducirá en el seno de las redes un modelo de desarrollo y cooperación comunitario en la producción de software que rompe con las dinámicas industrialistas (jerárquicas, ligadas al modelo empresa o Estado) y se inscribe o da forma a un modelo plenamente reticular, horizontal y comunitario que está en la base del nuevo paradigma informacionalista y en la estructura cromosómica del movimiento del software libre (Sádaba Rodríguez y Roig Domínguez, 2004).

Richard Stallman publicó el *Manifiesto GNU* en marzo de 1985, en la revista *Dr. Dobb's Journal of Software Tools*. Con este texto asentó los principios del Proyetco GNU, que significa "GNU's Not Unix" ("GNU No es Unix") y da nombre al sistema operativo libre y completamente compatible con Unix que Stallman escribió, junto con algunos voluntarios, siguiendo el diseño tipo Unix, pero con software libre.

Básicamente, en su manifiesto Stallman expresa su crítica al sistema comercial que permite a los fabricantes de software privativo "dividir a los usuarios y dominarlos para llevarlos a aceptar que no pueden compartir su software con los demás" (Stallman, 1985). Frente a este sistema autoritario y privativo, propone un modelo basado en una producción cooperativa, libre y abierta; un modelo productivo opuesto a la apropiación de las fuentes de innovación y de la producción de conocimiento.

[59] Aunque *Neuromancer* es la primera gran obra publicada donde se habla del ciberespacio, Gibson acuñó antes el término en su relato *Johnny Mnemonic*, publicado en mayo de 1981 en la revista neoyorkina de ciencia y ciencia ficción *Omni* —que se publicó entre 1978 y 1998—, e incluido en la colección *Burning Chrome* (1986) de relatos de ficción de Gibson.

> Los acuerdos que obligan a la gente a pagar por usar un programa, incluyendo la licencia de las copias, siempre incurren en un coste enorme para la sociedad por los aparatosos mecanismos necesarios para determinar cuánto —es decir, qué programas—debe pagar una persona. Y sólo un estado policial puede forzar a todo el mundo a obedecer. Considere la posibilidad de una estación espacial en donde el aire debe fabricarse con un gran coste: cobrar a cada persona por litro de aire quizá sea justo, pero usar una máscara para medir el aire durante todo el día y toda la noche sería insoportable, incluso aunque todo el mundo pudiese permitirse el lujo de pagar la factura de su consumo de aire. Y tener cámaras de video en todas partes para ver si alguna vez alguien se quita la máscara sería indignante. Es mejor costear la planta de aire con un impuesto y desechar las máscaras. Copiar todo o parte de un programa es tan natural para un programador como respirar, y además es productivo. Debería ser algo libre (Stallman, 1985).

Por último, en 1984 se empezó a escribir la génesis de lo que una década después se bautizó como hacktivismo. Aquel año, algunas organizaciones no gubernamentales empezaron a descubrir el potencial de la computación para la defensa de causas sociales, consituyendo la primera red computacional global para los movimientos civiles en el marco del proyecto Interdoc, surgido del Acuerdo Valletri, por el cual varias organizaciones no gubernamentales de cuatro continentes acordaron utilizar líneas telefónicas internacionales para enlazar sus computadoras.

Al mismo tiempo, en Estados Unidos una nueva generación de jóvenes hackers empezó a organizarse en distintos grupos que se manejaron en el *underground* informático y que llevaron la ética hacker hacia posiciones más radicales. Uno de ellos fue Legion of Doom, uno de los colectivos hackers más famosos e influyentes en el mundo, activo hasta principios del siglo XXI y convertido en mito, principalmente por haber sido el primer gran objetivo de las redadas policiales contra los hackers en Estados Unidos, aunque si por algo quisieron darse a conocer fue por su labor de divulgación. Ese mismo año también nació el primer grupo hacktivista de la historia, Cult of the Dead Cow, y con éste, su *paramedia online*, considerado por muchos hackers el primer *e-zine* en Internet (revista electrónica).

Cult of the Dead Cow se fundó en 1984 como un proyecto experimental hacker para exprimir habilidades computacionales, artísticas y satíricas. En la década de 1990, este grupo empujó a parte de la comunidad hacker al activismo y abrió nuevos escenarios sociopolíticos en la Red, con el objetivo principal de aplicar la Declaración Universal de Derechos Humanos a Internet, además de defender el derecho a la información como un derecho humano fundamental. Diez años después de su

fundación, Cult of the Dead Cow acuñó el término *hacktivismo*, en 1994.

El año 1984 marcó un punto de inflexión en la historia hacker, en el mundo de la computación, en el activismo y en nuestra cultura determinada por las tecnologías digitales. Todos estos acontecimientos sucedidos aquel año, y la cada vez más relevante presencia de la comunidad hacker en los medios de comunicación de masas, *oficializaron* y elevaron al rango de nueva corriente cultural este movimiento que se encontraba en el epicentro de uno de los mayores avances tecnológicos en la historia de la humanidad y de una nueva era, la de la sociedad red.

I.4.5. Éxtasis hacker

La década de 1980 fue la del éxtasis hacker y la de su definitiva configuración como cultura. En el ocaso de los años ochenta del pasado siglo se produjo uno de los más recordados acontecimientos mundiales entre la comunidad hacker global: la Galactic Hacker Party. La reunión tuvo lugar entre el 2 y el 4 de agosto de 1989 en el centro cultural Paradiso de Amsterdam e impulsó la celebración de una serie de encuentros de hackers cada cuatro años: Hacking At The End Of The Universe (1993), Hacking In Progress (1997), Hackers At Large (2001), What The Hack (2005), Hacking At Random (2009) y Observe. Hack. Make (2013). La Galactic Hacker Party pasó a los anales hackers en letras de oro por reunir por primera vez a representantes de tres grupos clave en el desarrollo de la cultura hacker en Estados Unidos y Europa: el Chaos Computer Club (Alemania) y las revistas *Hack-Tic* (Holanda) y *2600* (Estados Unidos).

> La Galactic Hacker Party pudo muy bien haber sido el encuentro más extraño de hackers que jamás se haya montado. No fue solamente una reunión de *cabezas de silicio* que hablaron binario durante tres días. No era simplemente un grupo de individuos revoltosos sueltos para dar un quebradero de cabeza a las autoridades y causar un caos general donde fuese que se aventurasen. Tampoco era simplemente un grupo de tipos extraños, locos y ultraparanoicos, como los que llegan a las reuniones mensuales de *2600* en Nueva York. La Galactic Hacker Party fue una mezcla de estos tres tipos de grupos, y bastante más (Goldstein: 2009: 217).

La celebración de grandes conveciones de hackers en Europa inspiró a los miembros de esta comunidad en Estados Unidos, donde las reuniones eran herméticas, en formato de pequeñas conferencias para grupos reducidos, como Summercon, Def

Con, HoHoCon o la tradicional y anual Hackers' Conference californiana. En el verano de 1994, con motivo del décimo aniversario de la revista *2600*, sus responsables, imitando a sus colegas de la revista holandesa *Hack-Tic* —organizadores del Hacking at the End of the Universe (1993), recordado por muchos como el Woodstock hacker (Goldstein, 2009: 271)— organizaron en el Hotel Pennsylvania de Nueva York la primera gran convención internacional hacker en Estados Unidos, la primera reunión masiva de expertos en *hacking* en la cuna del *hacking*.

Alrededor de mil quinientos hackers de Estados Unidos, Alemania, Holanda, Italia, Canadá, Australia, Rusia, Israel o Argentina participaron los días 13 y 14 de agosto de 1994 en el primer evento hacker global, multidisciplinar y abierto celebrado en territorio estadounidense, bautizado como Hackers on Planet Earth (HOPE[60]). El encuentro tuvo su momento *mágico* cuando la audiencia escuchó vía telefónica, conectado desde una prisión, a un ilustre de la comunidad hacker, Phiber Optik (Goldstein, 2009: 276), por entonces incondicional del grupo hacker Masters of Deception, fundado a finales de la década de 1980 en Nueva York y que en 1990 contabilizaba catorce miembros.

Los encontronazos de Phiber Optik con la justicia comenzaron en enero de 1990, con los primeros coletazos de la *Operación Sun Devil* para desarticular a las principales organizaciones hackers de Estados Unidos. Tras la caída del sistema telefónico de AT&T el 15 de enero de 1990, en el Día de Martin Luther King Jr., Phiber Optik —cuyo nombre real es Mark Abene— fue por primera vez detenido y se le confiscó todo su material informático el 24 de enero 1990. Junto con él también fueron arrestados otros dos hackers de Masters of Deception apodados Acid Phreak (Elias Ladopoulos) y Scorpion (Paul Stira). Posteriormente, se demostró que la caída del sistema se debió a un fallo del software de la empresa y que ningún hacker tuvo nada que ver en aquel incidente, pero aquello contribuyó a alimentar aún más las paranoias y el pánico de las autoridades sobre los hackers. Tras no haber podido presentar cargos contra Phiber Optik, las autoridades federales del estado de Nueva York volvieron a la carga un año después.

En febrero de 1991, Phiber Optik fue arrestado, acusado de manipular ordenadores, de allanamiento informático en primer grado y de una falta de robo de

[60] El acrónimo es la palabra inglesa *hope*, que en español significa esperanza.

servicio por no pagar llamadas telefónicas. Phiber Optik solamente se declaró culpable de este último delito y fue sentenciado a treinta y cinco horas de trabajos comunitarios. En diciembre de ese mismo año fue arrestado una vez más, en plena campaña de acoso y redadas a los hackers por el caso AT&T, y fue acusado en julio de 1992 de once delitos, de los cuales se declaró culpable de dos: conspiración y acceso no autorizado a computadoras de interés federal. El acto de conspiración de Phiber Optik fue facilitar información a un amigo de cómo desviar una llamada y acceder a la página de Educational Broadcasting Company para dejarles un mensaje; el acceso no autorizado a computadoras de interés federal se definió como acceso no autorizado a ordenadores de Southwestern Bell, provocando supuestos daños valorados en 370.000 dólares. Responsables de la propia Southwestern Bell reconocieron que no se había causado daño alguno. La Fiscalía pidió cincuenta años de cárcel y dos millones y medio de dólares de multa para el hacker. Finalmente, Phiber Optik fue sentenciado el 3 de noviembre de 1993 a un año y un día de prisión en una cárcel federal, seiscientas horas de servicio comunitario y tres años de libertad condicional supervisada. También sus compañeros Acid Phreak y Scorpion fueron condenados a seis meses de arresto domiciliario, setecientas cincuenta horas de servicio comunitario y multa de cincuenta dólares por conspiración para cometer crimen mediante computadoras.

En enero de 1994, Phiber Optik empezó a cumplir su condena por conspiración como miembro de Masters of Deception y por acceder ilegalmente a computadoras de interés federal. Sus vínculos con Emmanuel Goldstein eran muy estrechos, no en vano, había participado tanto en la revista *2600* como en el programa de radio de Goldstein *Off the Hook*. Su condena fue declarada por el propio juez un mensaje de advertencia a los hackers. Tras diez meses en la prisión del condado de Schuylkill, en Pennsylvania, salió en libertad como un auténtico héroe hacker. Pero a ojos del Departamento de Justicia de Estados Unidos era una persona subversiva.

Phiber Optik fue un hacker que abrió un nuevo camino a la comunidad, dando un paso en solitario al frente para mostrarse ante la sociedad y divulgar entre el gran público el conocimiento y la ética hacker y cualquier información tecnológica útil para los usuarios, en conferencias, cursos, medios de comunicación… "No tuvo miedo a exponerse en público y mostrar a la gente qué era exactamente aquello de lo que hablaba. […] Phiber Optik fue uno de los primeros hackers en quitarse la máscara y

presentarse con información." (Goldstein, 2009: 526-527). La suya fue una actitud subversiva a ojos de la autoridad y transgresora a los de la comunidad hacker. Hoy, Phiber Optik es un reputado experto asesor en seguridad informática y un mito viviente en la cultura hacker, cuya historia y la de sus colegas de Masters of Deception y Legion of Doom fue retratada en el polémico libro *Masters of Deception: The Gang That Ruled Cyberspace* (HarperCollins, 1995), de Michelle Slatalla y Joshua Quittner, en plena efervescencia del *hacking* en la cultura popular de masas.

Otro de los casos que también adquirió gran fama en la comuniad hacker fue el de Craig Neidorf, editor de la revista *Phrack*. Su caso se desarrolló a la par que el de Phiber Optik y se enmarca en la campaña a gran escala que las autoridades estadounidenses emprendieron contra la comunidad hacker en 1990. Neidorf, conocido como Knight Lightning, manejaba una BBS llamada Metal Shop. Junto a sus amigos Cheap Shades y Taran King, editaba la publicación electrónica *Phrack*. Esta versaba sobre temas relacionados con el *hacking* y el *phreaking*, la anarquía o las comunicaciones mediadas por las tecnologías. La copia y publicación en febrero de 1989 en *Phrack* de un documento del sistema de la línea de emergencias E911 (o Enhanced 911) convirtieron a Neidorf y a su publicación en objetivo del Servicio Secreto. El documento había sido copiado de las computadoras de BellSouth en diciembre de 1988 por The Prophet, miembro del grupo hacker Legion of Doom, colaboradores de la revista *Phrack*. El 18 de enero de 1990 —tres días después de la caída nacional del sistema telefónico de AT&T el Día de Martin Luther King Jr.—, el Servicio Secreto inició su acoso a Neidorf, a quien incluso se le acusó en un primer momento de haber participado en el incidente de AT&T, en el que luego fueron implicados Phiber Optik, Acid Phreak y Scorpion. A las detenciones en Nueva York de los tres hackers de Masters of Deception se sumaron los arrestos de miembros de Legion of Doom y de Neidorf en febrero de 1990. A éstos se les imputaron siete cargos, incluido el de traficar con información robada entre Estados. The Mentor, uno de los miembros más destacados de Legion of Doom, publicó una declaración de defensa del grupo en la que, entre otros aspectos, destacó:

> He conocido a la gente involucrada en este caso 911 durante muchos años, y no había absolutamente ninguna intención de interferir o molestar el sistema 911 de ninguna manera. Aunque en alguna ocasión hemos entrado en equipos en los que se suponía que no debíamos estar, es motivo de expulsión del grupo y de ostracismo social causar cualquier daño a un sistema o intentar cometer fraude con fines de lucro

> personal. El mayor crimen que se ha cometido es el de la curiosidad… Hemos sido fundamentales en el cierre de muchos agujeros de seguridad en el pasado y teníamos la esperanza de continuar haciéndolo en el futuro. La lista de personas del mundo de la seguridad informática que nos tienen como aliados es larga, pero debe permanecer en el anonimato. Si alguno de ellos opta por identificarse, agradeceríamos su apoyo (Goldstein, 2009: 497).

Neidorf fue acusado de hacer peligrar el sistema de asistencia más grande del país y de poner en riesgo muchas vidas, afectando la confianza general de los ciudadanos en este sistema de emergencias. En el caso de Neidorf, abogados de la Electronic Frontier Foundation presentaron una copia del polémico documento E911, adquirida en una oficina común y corriente de la Bell por solamente dos dólares, demostrando que el texto en cuestión era público, barato y que no podía considerarse importante de ninguna manera. Pero, sobre todo, los abogados intentaron remarcar el hecho de que la confiscación de los equipos sobre los que funcionaba *Phrack* suponían un daño tan grave a la libertad de prensa como si a un diario se le clausuraran las imprentas. Los cargos, finalmente, fueron retirados por aportación de información falsa por parte de Bell South a la Fiscalía. El documento que se afirmaba que tenía un valor de 79.449 dólares resultó finalmente tener un valor real de tan sólo trece dólares (Sterling, 1992; Goldstein, 2009: 501).

La moraleja de aquel caso fue la que suele emerger en otros similares: "Echar la culpa a los hackers por encontrar las fallas es otra manera de decir que las fallas deben permanecer inadvertidas" (Goldstein, 2009: 500). Lo cierto es que no se había causado ningún daño real al sistema y, además, se había evidenciado la existencia de grandes agujeros de seguridad que a su vez demostraban la mala calidad en el diseño de un sistema tan importante como el E911. Sin embargo, este aspecto del caso fue esquivado por las autoridades y por los medios de comunicación tradicionales.

Otro caso paradigmático del acoso político, policial y judicial al que fueron sometidos los hackers a finales de los años ochenta y durante la década de 1990 fue el de Edward Cummings, conocido en la comunidad hacker como Bernie S., también colaborador de la revista *2600*, como Phiber Optik. Cummings fue acusado en 1995 de poseer un marcador de teléfono modificado (una caja roja[61]) y un ordenador con

[61] Una caja roja es un dispositivo usado por *phreakers* que emite tonos iguales a los que envían a sus centrales los teléfonos públicos de pago cuando se introducen monedas, resultando la comunicación gratis.

software para manipular y modificar sistemas telefónicos. Por ello cumplió condena en la cárcel desde el 14 de marzo hasta el 13 de octubre de 1995, cuando salió en libertad condicional. El 12 de enero de 1996, en la vista oral de su libertad condicional, se le acusó de manipular pruebas por quitar las pilas a un marcador de teléfono, cosa que en realidad hizo un amigo suyo. Además, un agente del Servicio Secreto, Tom Varney, declaró ante el juez que consideraba a Cummings un gran riesgo para la sociedad, ya que durante un registro en la casa del hacker habían encontrado, entre otros materiales, un listado de frecuencias y códigos del Servicio Secreto disponibles libremente en Internet, una sustancia que parecía explosivo plástico C4 (aunque reconoció que en realidad tan sólo era material de dentistas para hacer empastes) y un ejemplar del libro *The Anarchist Cookbook*[62]. Por ello fue enviado a prisión hasta el 13 de septiembre de 1996 y se le impuso una fianza de 250.000 dólares. El mismo día, el mismo juez puso una fianza de 50.000 dólares a una persona reincidente que había atropellado y matado a otra mientras conducía ebria.

Durante el tiempo que Cummings pasó en prisión —en diferentes centros, la mayoría de máxima seguridad— fue apaleado por otro prisionero, se le negaron analgésicos y medicación, y fue encerrado en una celda de aislamiento la mayor parte del tiempo. Todo, oficialmente, por quitar una pila a un marcador de teléfonos. Cummings argumentó más tarde que la verdadera razón de su castigo fue que publicó en su sitio web las imágenes de dos agentes del servicio secreto registrando su oficina, uno de ellos metiéndose el dedo en la nariz. Ese agente era precisamente Tom Varney. Esas imágenes aún están disponibles en la página web de la revista *2600*.

---

[62] *The Anarchist Cookbook* es un manual escrito en 1969 por William Powell —quien por entonces tenía 19 años— y publicado en 1971 por el editor independiente Lyle Stuart. Powell decidió escribir el libro tras recibir una carta de reclutamiento para combatir en Vietnam. A modo de venganza y protesta, escribió este libro basándose en manuales militares, con instrucciones dispares sobre cómo desarrollar técnicas de contravigilancia, cultivar drogas, utilizar armas, crear gas lacrimógeno o manejar explosivos. El libro ha generado múltiples controversias, procesos judiciales y querellas, pero también ha sido definido como un fruto de la contracultura estadounidense de finales de la década de 1960 y primera mitad de 1970. Se convirtió, además, en todo un fenómeno de distribución entre la población mediante copias, pasando de mano en mano sin que las autoridades estadounidenses pudiesen hacer nada por evitarlo. Con la aparición de las primeras BBS el manual se comenzó a distribuir digitalmente en modo texto y, otros muchos años después, en formato PDF descargable en Internet. Pasado el tiempo, su autor promovió campañas contra su propio texto. Pero Powell —convertido al anglicanismo y dedicado a la educación de niños pobres de África y Asia— había vendido los derechos del libro. El editor, conocedor del potencial comercial de la obra —se calcula que se han vendido unos dos millones de ejemplares— se negó a retirarla. Lo amparaba la Primera Enmienda de la Constitución estadounidense. Grupos anarquistas como CrimethInc han renegado de este manual, ya que consideran que ni proviene de la práctica anarquista ni está destinado a promover la libertad y la autonomía o a desafiar el poder represivo. El libro puede ser adquirido en Internet a través de plataformas como Amazon.

Ilustración 5: Imágenes publicadas por el hacker Edward Cummings de agentes del Servicio Secreto de Estados Unidos.

Fuente: http://www.2600.com/secret/more/photo.html.

El 7 de septiembre, Cummings, en sus propias palabras, "se vio obligado a hacer un trato con el diablo". Se declaró culpable de posesión de tecnología que se podría utilizar con fines fraudulentos. Es decir, la mera posesión es igual a un uso fraudulento, en virtud de una nueva ley federal que acababa de ser aprobada[63], aunque Cummings nuna fue acusado de cometer fraude; "un giro muy inquietante" para los hackers, ya que prácticamente cualquiera interesado en el *hacking* informático o en el sistema telefónico podría ser enviado a prisión y ser tratado como un terrorista (Goldstein, 2009: 537-538).

El caso de Cummings motivó una de las primeras grandes acciones en red colaborativas como protesta en la comunidad hacker.

> En una acción sin precedentes, los visitantes del sitio web *2600*, los radioyentes de *Off The Hook* de WBAI y hackers alrededor de todo el planeta unieron sus fuerzas para poner fin a la pesadilla de una vez por todas. Se abrió una lista de correo que rápidamente consiguió cientos de suscriptores. Se estableció una línea directa de correo de voz en *2600*. Voluntarios trabajaron noche y día. Personas que nunca habían formado parte del mundo hacker comenzaron a involucrarse. Estaba claro que esto ya no era una cuestión de hackers, sino más bien un caso significativo sobre derechos humanos. Incluso miembros de los medios de comunicación comenzaron a interesarse por ello (Goldstein, 2009: 542-543).

El 13 de septiembre de 1996, la pesadilla terminó. Ed Cummings, que había sido encerrado en una prisión de alta seguridad con delincuentes condenados por actos violentos y que sufrió penalidades en la cárcel, fue puesto en libertad de manera inmediata y se convirtió en un "claro ejemplo del poder el pueblo". Quince años antes

63 Véase *18 U.S. Code § 1029 - Fraud and related activity in connection with access devices*, en https://www.law.cornell.edu/uscode/text/18/1029 (último acceso: 11 de septiembre de 2014).

de que los *indignados* españoles parecieron descubrir el poder de la indignación y catorce años antes de que Stéphane Hessel publicase el libro *¡Indignaos!* como preludio *profético* del movimiento civil español, la comunidad hacker ya había canalizado y convertido en poder político la energía generada en la indignación colectiva: "La mera preocupación no es realmente suficiente. Al final, sólo la verdadera indignación obtiene resultados" (Goldstein, 2009: 544).

El caso de Cummings también abrió grietas entre la revista *2600* y las organizaciones por las libertades civiles, a las que acusó de ser cómplices del Servicio Secreto de Estados Unidos con su silencio: "No hemos oído ni una palabra sobre este caso de Electronic Frontier Foundation, American Civil Liberties Union, Computer Professionals for Social Responsibility o Electronic Privacy Information Center" (Goldstein, 2009: 537).

Los casos de Edward Cummings y Phiber Optik no fueron aislados. En la cultura hacker se recuerdan también otras persecuciones que pasaron a la historia de esta comunidad como paradigmáticas de la presión a la que el Estado-nación estaba sometiendo a quienes estaban liderando la vanguardia en el uso de las nuevas tecnologías. El de Kevin Mitnick fue uno de ellos.

Mitnick —*phreak* experto en ingeniería social, seguridad informática y análisis de sistemas— estuvo cinco años en prisión por, supuestamente, haber accedido a ordenadores de empresas estadounidenses y haber causado millones de dólares en daños que nadie fue capaz de probar. Kevin Mitnick solamente quería aprender cómo funcionaban los sistemas en los que había penetrado. Su juicio comenzó el 10 de julio de 1995 en Raleigh, Carolina del Norte. Se enfrentó a una acusación de veintitrés cargos federales, cada uno de los cuales conllevaba una sentencia de veinte años de prisión. Se declaró culpable de uno. Como en el caso de Cummings, de nuevo la acción en red se puso en marcha para la protesta. El 4 de junio de 1999 se convocaron manifestaciones en defensa de Mitnick por todos los Estados Unidos, frente a los juzgados federales. Emmanuel Goldstein describe así aquella contestación civil, ya en plena efervescencia hacktivista:

> Estamos viendo un cantidad de activismo sin precedentes en la comunidad hacker y la razón es simple. Esto es demasiado como para ser tolerado. No podemos permitir que este sufrimiento continúe. Y aquéllos que se mantienen en silencio son tan culpables como los que animan a este tipo de abuso (Goldstein, 2009: 549).

Lo cierto es que a Mitnick no sólo se le privó de su libertad, también se le mutiló intelectual y profesionalmente, incluso socialmente, imponiéndole durísimas restricciones para concederle la libertad supervisada. Durante tres años, Mitnick no podría poseer o usar para cualquier propósito ningún equipo de hardware, programa de software, módem ni equipos periféricos o equipos de apoyo, computadoras portátiles, asistentes personales de información y derivados, teléfono móvil, televisor o instrumentos de comunicación equipados con línea de Internet, World Wide Web u otro tipo acceso a la red informática. Tampoco podría utilizar equipo electrónico alguno ni ninguna tecnología que se pudiese convertir en o tuviese capacidad para actuar como un sistema de computación. También se le prohibió acceder a cualquier sistema informático, red informática o red de telecomunicaciones, ni a ninguna tecnología inalámbrica de comunicación, ni siquiera través de terceros. Sólo se le permitió el uso del teléfono fijo,

Entre las medidas disciplinarias que se le aplicaron a Mitnick se incluyeron la prohibición de ser empleado o realizar los servicios para cualquier entidad dedicada a la computación, el desarrollo de software o el negocio de las telecomunicaciones ni, en cualquier calidad, en ningún negocio que le pudiese ofrecer acceso a computadoras o equipos relacionados con la informática o software. Las restricciones temporales no terminaron ahí. Además, se le imposibilitó a ejercer como consultor o asesor de individuos o grupos comprometidos en cualquier actividad relacionada con computadoras y no podría adquirir ni poseer ningún código informático, incluyendo contraseñas de computadoras y códigos de acceso a teléfonos móviles o a otros dispositivos que le permitiesen usar, adquirir, intercambiar o alterar la información en una computadora o en una base de datos. Tampoco se le permitió usar o poseer tecnología de encriptación de datos, ni modificar teléfonos o poseer un equipo alterado, ni podría utilizar cualquier teléfono o equipo telefónico con otro fin que no fuese hablar directamente con otra persona. Por último, sólo podría utilizar su verdadero nombre y se le prohibió usar más un alias u otra identidad falsa o pseudónimo (Goldstein, 2009: 564).

Tras cinco años en prisión, Mitnick describió lo absurdo e irrazonable de la condena en una carta publicada en la edición de primavera de 2000 en la revista *2600*, en agradecimiento al apoyo prestado por esta publicación y la comunidad hacker:

> Si incluso utilizase una computadora para comprar una Metrocard para viajar en el sistema de metro de Nueva York, también estaría violando las condiciones de la libertad condicional. Esas condiciones también restringen mis derechos de la Primera Enmienda en la medida en que se me prohíbe actuar como asesor de cualquier persona que se dedica a actividades relacionadas con la computación. Mi reciente charla en el Senado podría ser una violación de la condicional, como lo podría ser también una charla a un mecánico de coches. Las condiciones son tan vagas y excesivamente amplias que no sé qué tengo que hacer o no hacer para mantenerme fuera de la cárcel. Que vuelva o no a prisión depende de lo que decida un funcionario del Gobierno, y no se basa en mis propósitos, es algo completamente arbitrario (Mitnick, en Goldstein, 2009: 586).

La odisea carcelaria de Mitnick comenzó el 15 de febrero de 1995, pero antes había vivido como fugitivo durante dos años y medio para evitar ser de nuevo capturado, como sucedió en 1988, cuando fue castigado a ocho meses de confinamiento, encarcelado en régimen de incomunicación absoluto, tras las alegaciones del fiscal, que había convencido al juez de que Mitnick tenía la extraordinaria habilidad de iniciar una guerra nuclear marcando un teléfono e introduciendo un código, algo nunca demostrado. Todo cuanto había hecho Kevin Mitnick, años atrás, en 1979, había sido penetrar en el sistema de computadoras The Ark, de la empresa Digital Equipment Corporation, el cual era usado para desarrollar el software del sistema operativo RSTS/E. Según cuenta el propio Mitnick en el libro *The Art of Deception*, su acción respondió al desafío que le habían planteado unos hackers a los que conocía y quería impresionar para formar parte de su grupo. Una vez que Mitnick les demostró que había superado el reto, los otros hackers utilizaron los datos de acceso que había conseguido Mitnick y copiaron el código fuente del sistema operativo RSTS/E (Mitnick y Simon, 2002). Aquella fue la primera gran experiencia hacker de Mitnick, con 16 años de edad.

Pero la primera de las incursiones que llevaron a Mitnick a la categoría de mito en la comunidad hacker se produjo dos años después, cuando él y dos amigos se colaron en el Computer System for Mainframe Operations (COSMOS) de la compañía Pacific Bell —que era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de llamadas— y obtuvieron el listado de claves de seguridad, combinaciones de acceso de varias sucursales y diversos manuales de COSMOS. El valor total de la información obtenida por Mitnick y sus colegas se calculó en unos 150.000 dólares. Su acción le costó su primera condena: tres meses de prisión y un año de libertad vigilada. La sentencia fue dictada

por un tribunal de menores. En 1983, Mitnick —que se hizo llamar The Condor en los círculos hackers— volvió a ser arrestado por utilizar un ordenador de la University of Southern California para obtener acceso no permitido a la red ARPAnet e introducirse en un ordenador del Pentágono. Por ello fue sentenciado a seis meses de cárcel en una prisión juvenil del estado de California.

Ya en el año 1987, Kevin Mitnick fue acusado de robar software de Microcorp Systems, una pequeña empresa californiana, y fue condenado a tres años de libertad condicional, con la prohibición de usar computadoras. Pero Mitnick no dejó de incursionar en equipos informáticos de otras organizaciones. Lenny DiCicco, un amigo con quien había trabajado en la consecución de un sistema operativo del laboratorio digital de Palo Alto (California), lo delató el año siguiente. Mitnick fue detenido y acusado de entrar en la red de la Digital Equipment Corporation y de robar código fuente de ésta. Esta vez tuvo que pasar un año de cárcel. Su abogado impidió una condena mayor alegando que Mitnick tenía una adicción a su equipo informático. Se trataba de la quinta ocasión en que Mitnick había sido arrestado por un caso de crimen informático y el caso atrajo la atención de la toda la nación, gracias a la inusual táctica de la defensa y a los argumentos esgrimidos por el FBI y el fiscal, a los que DiCicco había hecho creer que Mitnick estaba suficientemente cualificado para iniciar remotamente una guerra nuclear.

Ilustración 6: Orden de búsqueda contra el hacker Kevin Mitnick.

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132 (Rev. 3/2/92)

November 1992

Fuete: http://www.extremetech.com/.

A finales de 1989. Kevin Mitnick fue puesto en libertad y comenzó a trabajar recopilando información para investigadores privados, iniciando una vida cuasi nómada que le llevaría por distintos Estados de la nación y a protegerse con falsas

identidades por miedo a tener que enfrentarse de nuevo con la justicia. Mitnick accedió a redes de Motorola, Sun Microsystems, Nokia y Novell, entre otras. Su fama creció, en los medios de comunicación se le trató como terrorista cibernético, se convirtió en uno de los fugitivos más famosos del país y logró convertirse en el centro de atención del FBI. El 15 de febrero de 1995, el FBI finalmente atrapó a Mitnick. El juicio contra el hacker se retrasó por más de cuatro años, tiempo en el que fue retenido sin derecho a libertad bajo fianza. El 20 de enero de 2000, Mitnick salió en libertad vigilada por tres años, lo que suponía de facto quince años sin libertad, sin haberse lucrado ni robado ni causado daño alguno, castigado por haber hecho unas llamadas telefónicas gratuitas y acceder a un código fuente ajeno (Goldstein, 2009: 575, 597).

Kevin Mitnick —quien fue considerado por la autoridad el hacker más peligroso del mundo y por la propia comunidad hacker, su miembro más brillante e importante— es hoy toda una celebridad mundial en el mundo de la seguridad informática y de la ingeniería social. Su figura ha pasado a ser parte de la cultura popular estadounidense. Mitnick se dedica actualmente a la consultoría con su empresa, Mitnick Security. En su página web —https://www.mitnicksecurity.com/— aún presume de haber sido "una vez una de las personas más buscadas por el FBI porque hackeó cuarenta grandes corporaciones solamente por el reto" que suponían esas incursiones. Ahora se describe como un "consultor de seguridad de confianza para las empresas de Fortune 500[64] y gobiernos en todo el mundo". Mitnick también ha escrito importantes libros sobre seguridad informática —*Art of Deception: Controlling the Human Element of Security* (2002) y *Art of Intrusion: The Real Story Behind the Exploits of Hackers, Intruders and Deceivers* (2005)— y una autobiografía titulada *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* (2011).

En la década de 1990, a la vez que el *hacking* adquirió pleno significado político, la cultura hacker fue arrojada a los circuitos comerciales y de la cultura popular de masas. En estos años, el retrato robot del hacker creado por el poder y difundido por los medios de comunicación de masas se volvió "más siniestro" (Goldstein, 2009: 524) y las detenciones de hackers aumentaron significativamente. Pero también más y más miembros de esta cultura fueron fagocitados por empresas

[64] La lista Fortune 500 es publicada anualmente por la revista *Fortune* e incluye las quinientas mayores empresas estadounidenses de capital abierto a cualquier inversor según su volumen de ventas.

para el desarrollo de sistemas de seguridad o de software, debido al propio desarrollo de la Red de redes. "Muchos de los hackers de los años 80 fueron los programadores o diseñadores de la década de 1990" (Goldstein, 2009: 277). Por otro lado, el avance de Internet, de las comunicaciones en red e inalámbricas, y de una nueva industria de las tecnologías de la información y la comunicación permitieron el desarrollo de nuevas comunidades y estrategias hackers y una reconceptualización de esta cultura, con cada vez más activistas dispuestos a usar sus detrezas en pro de causas sociales y políticas. Información sobre sistemas informáticos, sistemas telefónicos, regulaciones gubernamentales, abusos de privacidad y nuevos *juguetes* tecnológicos fluían libre y abiertamente.

Al mismo tiempo, el cine y la televisión encontraron en la criminalizada figura del hacker una caudalosa fuente de historias que vender sobre jóvenes rebeldes y delincuentes apasionados de las computadoras, los *villanos* de la era computacional, los forajidos de un nuevo mundo ciberespacial y en red aún en estado salvaje. Esto no fue algo extraordinario. La hacker no era la única cultura *underground* arrojada a las masas para ser devorada por estas en un aquelarre consumista y banal, ni era tampoco la única respuesta de resistencia a la alienación de masas; el comercialmente sellado movimiento musical *grunge*, enraizado en Seattle, estaba siendo por entonces también servido a las masas como producto mercantil del momento. Contracultura engullida por la cultura alienante de masas y condenada a la fugacidad y transitoriedad de las modas. El discurso social y político radical y contestario de aquellos jóvenes músicos que, como los hackers, proyectaban una imagen y un estilo de vida radicalmente contrarios a los convencionales (Nirvana, Pearl Jam, Mudhoney, Soundgarden, Alice in Chains…), fue transfigurado por el mercado capitalista en producto comercialpantalones rotos exhibidos en las pasarelas, camisas de leñador que inundaban los locales nocturnos de ocio en las ciudades, pelos desgreñados y poses combativas trazados milimétricamente por departamentos de márketing y diseño en revistas de moda… De igual modo, la cultura hacker empezaba a ser engullida por Hollywood.

> Fue en la década de 1990 cuando los hackers fueron realmente descubiertos en el *mainstream*. Por supuesto que había un puñado de libros y películas de la década de 1980, pero eso no fue más que un preludio de lo que estaba yendo a toda velocidad por Hollywood Boulevard y Madison Avenue. En el transcurso de un par de años fue como si una nueva forma de vida hubiese sido descubierta, y todos tenían que tener un

> pedazo de la historia, ya fuese para diseccionarnos o para atacarnos. Ser un hacker en la década de 1990 era como ser un miembro de una banda de *pop* británico en la década de 1960; había esa delirante aura que te rodea y de la que no te puedes desprender por mucho que lo intentes (Goldstein, 2009: 233).

El desarrollo y expansión de Internet fue decisivo para ampliar la percepción del hacker como una verdadera amenaza mundial. Esa amplificación por canales de ficción y entretenimiento, y de realidad, contribuyó a que "la gente empezase a ver paralelismos entre lo que sucedía en el mundo hacker y lo que pasaba en el mundo real" (Goldstein, 2009: 491).

La década de 1990 también despertó las primeras divisiones y enfrentamientos críticos entre hackers. Masters of Deception criticaba públicamente a Legion of Doom a la vez que ambos grupos recibían críticas de sectores hackers ortodoxos por sus acciones, su *modus operandi* y la mala imagen que, decían, estaban proyectando de la comunidad. Así se reconoce en un artículo publicado en la revista *2600* en verano de 1992, con el título 'Here We Go Again', donde se advierte del poder de los medios de comunicación de masas para conseguir convertir cualquier relato en verdad revelada y del peligro que para la comunidad hacker supone asumir por parte de algunos de sus miembros los argumentos difundidos por la autoridad para criminalizar a toda la comunidad hacker: "Al crear la apariencia de facciones en guerra, le damos permiso a los medios de comunicación para convertirlo en realidad. Una vez que lo hacen, ya no importa si fue o no cierto. Se convierte en verdad" (Goldstein, 2009: 526). En el centro de las desavenencias se encontraron la revista *2600* y la Electronic Frontier Foundation.

La creación de la Electronic Frontier Foundation abrió una nueva vía de activismo en el ciberespacio. Aunque no es en sí misma una organización hacker, su génesis como organización por la defensa de las libertades civiles está directamente ligada a la ética hacker.

La Electronic Frontier Foundation fue la primera organización de derechos civiles en el ciberespacio, la primera organización política en la red electrónica. Sus orígenes se encuentran en la primavera de 1990, cuando se desarrolló la *Operación Sun Devil*, el mayor golpe dado a la comunidad hacker hasta entonces —la primera operación a gran escala contra hackers—, que dejó una gruesa cicatriz en esta

comunidad durante años. Tras dos años de investigaciones, el gigantesco operativo se puso en marcha entre el 7 y 8 de mayo de 1990, cuando ciento cincuenta agentes federales, apoyados por oficiales locales, ejecutaron veintisiete órdenes de registro en distintas ciudades a lo largo de Estados Unidos para desmantelar a Legion of Doom. Un total de cuarenta computadoras y veintitrés mil discos fueron confiscados y numerosos tablones de anuncios electrónicos fueron cerrados. Barlow (1990) calcula que se perdió el equivalente digital a 5,4 millones de páginas de información. Aquellos acontecimientos fueron recogidos por Bruce Sterling en otra obra de referencia para la comunidad hacker: *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (1992).

El proceso, a cargo del Servicio Secreto de Estado Unidos, en cooperación con la oficina de la Fiscalía Nacional y el fiscal general del estado de Arizona, investigaba a los hackers por supuesto tráfico y abuso de números de tarjeta de crédito robados, códigos de discado de larga distancia y acceso no autorizado o daño a computadoras. La operación se llevó a cabo simultáneamente en Cincinnatti, Detroit, Los Ángeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San José y San Francisco (Sterling, 1992), y en ella cooperaron técnicamente las compañías de telecomunicaciones Pac Bell, AT&T, Bellcore, Bell South, MCI, US Sprint, MidAmerican, Southwestern Bell, NYNEX, US West y otras corporaciones que habían experimentado las intrusiones hackers.

La *Operación Sun Devil* fue fruto de dos años de investigaciones y su ejecución despertó airadas críticas por parte de líderes de los derechos civiles y de algunos congresistas, que acusaron y demostraron que el Gobierno había sobrepasado sus límites monitoreando un boletín electrónico y espiando correos electrónicos (Goldstein, 2009: 492). Varios grupos y representantes políticos y civiles empezaron a exigir aclaraciones y respuestas al Servicio Secreto y al FBI sobre la forma en que se llevaban a cabo estos procedimientos. Entre éstos, los más destacados fueron el congresista Don Edwards, del Subcomité de Derechos Civiles y Constitucionales, y la asociación Computer Professionals for Social Responsibility, que comenzaron a exigir a las agencias del Gobierno informes basándose en acuerdos y actas constitucionales sobre supervisión de las actividades investigativas gubernamentales. La respuesta fue pobre y poco clara, llegando a casos extremos, como las peticiones de información de

la Computer Professionals for Social Responsibility al FBI sobre los métodos de monitoreo de sistemas de tablones de anuncios y redes, con innumerables cartas no respondidas, evasivas y demoras, hasta que un año más tarde se les contestó que era probable que nunca tuviesen respuesta. Finalmente, y como reacción ante el operativo, surgió una nueva organización, la Electronic Frontier Foundation, liderada por Mitch Kapor, el fundador de Lotus Development Corporation y ON Technology; Steve Wozniak, cofundador de Apple y creador del primer Macintosh, y John Perry Barlow, letrista del grupo psicodélico Grateful Dead. La organización se orientó a trabajar sobre temas sociales y legales producidos por el impacto en la sociedad del creciente uso de las computadoras y los nuevos medios de difusión y distribución de la información. Su fundación es una de las primeras manifestaciones del activismo global y en red en el ciberespacio, aglutinadora de espíritus libertarios cuya actividad fue *in crescendo* a lo largo de la década de 1990.

> Antes de que te pudieras dar cuenta ya nos estábamos organizando y comunicando online de manera eficaz. A través de un sistema público UNIX en California conocido como The WELL[65] ayudamos a difundir la historia aún a más gente. Los medios de comunicación la recogieron. Creo que fue entonces cuando vi por primera vez el poder de la Red en la acción. Llovieron correos electrónicos, montones de personas querían saber lo que podían hacer y la palabra se extendió por todo el mundo. Entre los que expresaron su deseo de ayudar estaban el fundador de Lotus Mitch Kapor y el exletrista de Grateful Dead John Perry Barlow. Vieron aquellos acontecimientos como una razón para empezar un nuevo grupo que ayudaría a proteger a las personas de este tipo de injusticia. Y así, las semillas de la Electronic Frontier Foundation fueron plantadas (Goldstein, 2009: 492).

Durante la *Operación Sun Devil*, especialmente impactante y provocador para la comunidad hacker fue el caso de Steve Jackson, afamado diseñador de juegos de rol que fue acosado por el Servicio Secreto de Estados Unidos y su BBS para aficionados a sus juegos, intervenida. Jackson estaba trabajando en un nuevo juego basado en las novelas y cuentos de William Gibson, particularmente su obra *cyberpunk* más famosa, *Neuromancer*, fetiche entre buena parte de la comunidad hacker. El nuevo juego se llamaría *GURPS Cyberpunk*. Jackson contaba para su creación con la colaboración de The Mentor, miembro de Legion of Doom. Lo que Jackson no imaginó fue que las agencias federales estaban relacionando el término *cyberpunk* con la delincuencia computacional en plena efervescencia de la *Operación Sun Devil*. Como parte de ésta,

[65] The WELL (*The Whole Earth 'Lectronic Link)* era una BBS de la *Point Foundation,* fundación creada por el millonario libertario *Stewart Brand,* creador de la Hackers' Conference en San Francisco.

las oficinas de la empresa Steve Jackson Games, en Austin (Texas) fueron registradas sin previo aviso el 1 de marzo de 1990. Los agentes del Servicio Secreto confiscaron todo el equipo, incluida la computadora del BBS y las que se utilizaban para tareas administrativas, así como todos los borradores del manual del juego. Los agentes se llevaron cuatro computadoras que guardaban archivos de *GURPS Cyberpunk*, dos impresoras láser, cinco discos duros sueltos, más de trescientos discos de la empresa y gran cantidad de hardware diverso. También se allanó el hogar de The Mentor. El material no fue devuelto hasta finales de junio de aquel mismo año.

La excusa para tal intervención fue que, supuestamente, el libro —todavía sin terminar— sería un manual del hacker en el pleno significado peyorativo y criminal que las autoridades otorgan al *hacking*, es decir, una especie de tratado sobre cómo cometer fraudes y delitos con una computadora. Jackson —contra quien nunca se presentaron cargos— quedó prácticamente en la ruina, tuvo que despedir a gran parte del personal que trabajaba con él y sufrió continuos inconvenientes tras el secuestro de todos los registros administrativos, contables y de trabajo de su empresa (Barlow, 1990; Electronic Frontier Foundation, 1990).

Ese mismo año, poco después, la revista *2600* y la Electronic Frontier Foundation protagonizaron unas desavenencias inesperadas. En sus inicios, esta organización fue caracterizada en los medios de comunicación de masas como un "fondo de defensa hacker" y fue denostada por la gran industria de la computación comercial, aunque la Electronic Frontier Foundation se esmeró en marcar líneas rojas con los hackers informáticos para no ser introducida en la misma condena social. Sus intenciones, explicaron, eran educar a los responsables políticos, agentes de la ley y a la gente en general en la confluencia de las libertades civiles, la computación, las tecnologías digitales y las telecomunicaciones y sus implicaciones políticas (Goldstein, 2009: 502). La posición alejada de los hackers adoptada por la Electronic Frontier Foundation causó malestar en la idolatrada revista *2600*:

> […] nos resulta triste que hayan redirigido sus energías lejos de los hackers, porque es un área que tiene una enorme necesidad de intervención externa. Este verano ha habido un número sin precedentes de redadas del Servicio Secreto, con mucha gente bajo investigación simplemente por haber llamado a un tablón de anuncios. Y en al menos un caso se sacaron otra vez las pistolas a una persona de 14 años de edad. Esta vez, saliendo de la ducha. Nuestra opinión es que alguien tiene que manifestarse en contra de estas acciones y hablar en voz alta (Goldstein, 2009: 502).

Esta crítica a la Electronic Frontier Foundation, publicada en verano de 1990, contrasta con la defensa que anteriormente había hecho de esta organización la revista *2600*. Goldstein decidió desmitificarla y escribió un nuevo relato:

> […] es importante que quede claro qué es lo que está haciendo la EFF. Mucha gente tiene la suposición errónea de que el caso de Craig Neidorf fue financiado por el EFF y que fue en gran parte responsable de que éste se cayese. La propia EFF no ha dejado los hechos claros. Los principales medios de comunicación han transmitido la impresión de que todos los hackers están siendo ayudados por esta organización. Los hechos son los siguientes: la EFF presentó dos escritos en apoyo a Neidorf, ninguno de los cuales tuvo éxito. Mencionaron su caso bastante en sus comunicados de prensa, lo que ayudó a correr la voz. Fueron llamados por alguien que tenía información sobre el sistema 911 y éste fue remitido luego al abogado de Neidorf (esto difiere de sus afirmaciones de haber localizado un testigo experto). La EFF no ha dado ni un centavo a Neidorf. Al cierre de esta edición, su fondo de defensa asciende a 25 dólares. Y, aunque útil, su intervención legal realmente condujo a que Neidorf tuviese que pagar unos honorarios legales mucho más altos de lo que habría sido normal. Así, aunque que la presencia de la EFF es algo bueno, no podemos pensar en ellos como la solución al problema. No son más que un paso. Esperemos que haya muchos más. Si deseas involucrate con la EFF, te animamos a ello. Tu participación y entrada puede ayudarles a moverse en la dirección correcta (Goldstein, 2009: 502-503).

En primavera de 1991, la revista *2600* recibió con entusiasmo un nuevo viraje de esta organización hacia los hackers. El 1 de mayo de aquel año, la Electronic Frontier Foundation presentó una demanda civil contra el Servicio Secreto de Estados Unidos y contra otras personas involucradas en el acoso a Jackson y a su negocio un año antes. La demanda se interpuso en nombre de la empresa, del propio Jackson y de tres usuarios del BBS clausurado.

Steve Jackson ganó el caso y fue indemnizado con 50.000 dólares por los daños causados por el Servicio Secreto, derivados de su violación de la Ley de Protección de la Privacidad de 1980 (Privacy Protection Act), la cual protege a periodistas y editores de registros y de ser obligados a entregar material de trabajo periodístico y fuentes al Gobierno antes de su publicación. En la sentencia, hecha pública el 12 de marzo de 1993— se tuvo en cuenta que la acción de los agentes secretos había causado una importante pérdida de ingresos para la empresa de Jackson, hasta el punto de ponerla al borde de la bancarrota. El Gobierno de Estados Unidos también fue condenado a pagar los costes de la defensa de los demandantes y a indemnizar a cada uno con mil dólares, en base a la Ley de Privacidad de Comunicaciones Electrónicas de 1986 (Electronic Communications Privacy Act), que

prohíbe que los funcionarios encargados de hacer cumplir la ley puedan interceptar intencionadamente, utilizar y/o revelar el contenido de comunicaciones electrónicas privadas sin una orden judicial.

Los encontronazos de los hackers con el Servicio Secreto estadounidense fueron habituales en aquellos años decisivos para la configuración de Internet. Miembros de la revista *2600* y aficionados a ésta experimentaron el acoso de la autoridad el 6 de noviembre de 1992, durante un encuentro en el Pentagon City Mall de Arlington (Virginia). Una telectroniceintena de hackers se había reunido en unas mesas del área de hostelería del centro comercial; pronto fueron interrumpidos e identificados por los servicios de seguridad privada del centro comercial y policías locales de Arlington, y sus dispositivos electrónicos, cuadernos y otros artículos personales fueron requisados. Tres días después, Al Johnson, director de seguridad del Pentagon City Mall, reconoció al periodista Brock Meeks, del *Communications Daily*, que detrás de este asunto se encontraban el Servicio Secreto y el FBI. Aunque Johnson negó más tarde tales declaraciones, se hizo pública una grabación de la conversación (Goldstein, 2009: 514-515) que fue verificada por periodistas de *Newsbytes* y documentada por el Electronic Privacy Information Center. La repercusión del caso, movido por los hackers en redes electrónicas y medios alternativos, apareció en la portada de *The Washington Post* el 12 de noviembre de 1992, en un artículo que sugería la implicación del Servicio Secreto en aquella redada hacker (O'Harrow Jr., 1992).

Uno de los asistentes a aquella reunión organizada por la revista *2600* fue Craig Neidorf, el editor de *Phrack*, quien ya había experimentado los abusos de autoridad en nombre de la seguridad nacional. En el boletín publicado por *Computer Underground Digest* el 11 de noviembre de 1992 se recogen declaraciones de distintos testigos y participantes en la reunión y del propio Neidorf, quien explicaba así lo ocurrido:

> Vi a los agentes de seguridad fijándose en nosotros. Luego, comenzaron a venir hacia nosotros desde distintas direcciones bajo lo que parecía ser el mando de una persona con un *walkie-talkie* en un balcón. Cuando se acercaron, dejé el grupo y observé al personal de seguridad que rodeaba a unas treinta personas. El grupo estaba principalmente compuesto por estudiantes de secundaria y universitarios. Los guardias exigieron registrar las mochilas y bolsas de los asistentes a la reunión. Confiscaron

> material, incluyendo aplicaciones de CPSR[66], una copia de *Mondo 2000* (una revista) y otros materiales. También confiscaron la película a una persona que estaba intentando tomar fotografías de los guardias y se llevaron el lápiz y papel de un hacker llamado HackRat cuando éste intentó tomar nota de los nombres de los guardias (Meyer y Thomas, 1992).

Neidorf también explicó su convicción de que "la redada fue planeada", ya que los guardias de seguridad del centro comercial los identificaron como "hackers" y confesaron tener información sobre estas reuniones mensuales organizadas por la revista *2600*.

En la base de datos del Electronic Privacy Information Center existe documentación relativa a este caso, cuyos archivos fueron parcialmente desclasificados en 1996 por orden del Tribunal Federal de Apelaciones del 2 de enero de aquel año, tres años después de litigios entre el Servicio Secreto y la Computer Professionals for Social Responsibility y el Electronic Privacy Information Center, cuya demanda ante la Corte Federal se sostenía en la Ley de Libertad de Información (Freedom of Information Act) para la liberación de los registros del Servicio Secreto[67]. Los afiliados a la revista *2600* también recibieron respaldo legal de la Electronic Frontier Foundation y la American Civil Liberties Union.

El incidente del Pentagon City Mall ha sido descrito como un ejemplo de exceso de celo en las actividades policiales dirigidas contra los hackers informáticos. El caso planteó cuestiones hoy aún tan sustanciales y candentes en el debate público como la libertad de expresión y de reunión, la privacidad y la responsabilidad del Gobierno en la protección de estos derechos (*The 2600 Case*, s.f.). En el reporte publicado el 11 de noviembre de 1992 en el boletín electrónico semanal *Computer Underground Digest* se describía la actuación del Servicio Secreto como delictiva: "Si el Servicio Secreto de Estados Unidos estuvo involucrado en el uso de las fuerzas de seguridad privadas para perturbar a civiles, su acción parece no solamente superar su mandato, sino que además parece ser descaradamente ilegal" (Meyer y Thomas, 1992).

---

[66] Computer Professionals For Social Responsibility (CPSR) fue una organización global creada en Seattle (Estados Unidos) por científicos computacionales en 1981 para la promoción del uso responsable de la tecnología computacional. Estuvo representada en 26 países e incubó diversos proyectos, incluidos el Electronic Privacy Information Center. Su sitio web se mantiene en línea en la siguiente dirección: http://cpsr.org/ (último acceso: 10 de junio de 2014).

[67] Véase: https://epic.org/security/2600/DC_Cir_opinion.html (último acceso: 10 de junio de 2014).

Para los editores de *Computer Underground Digest*, los agentes secretos habían cometido un "intolerable y totalmente inaceptable abuso de autoridad y poder", lo cual demostraba que las autoridades habían "aprendido muy poco de los abusos de la *Operación Sun Devil*". No se trataba sólo de una "simple cuestión del ciberespacio", los abusos del Servicio Secreto planteaban "la cuestión de la relación entre las acciones de la policía del Gobierno y las libertades constitucionales que supuestamente nos protegen contra el injustificado control de derechos básicos". (Meyer y Thomas, 1992).

Unos meses antes de este incidente, el 8 de julio de 1992, cinco hackers habían sufrido otra redada. Los acusados eran conocidos en la comunidad hacker como Phiber Optik, Acid Phreak, Scorpion, Outlaw y Corrupt. Fueron acusados de delitos de conspiración, manipulación de ordenador, escuchas ilegales, fraude informático y fraude electrónico. La sustancialidad de este caso se encuentra en el método de investigación empleado por la autoridad: por primera vez en la historia, el Gobierno de Estados Unidos admitió el uso de escuchas telefónicas en una investigtación hacker como método de obtención de pruebas, lo cual situaba a los hackers en el mismo nivel de criminalidad que mafiosos y terroristas (Goldstein, 2009: 524).

Los encontronazos de la revista *2600* con la justicia también tuvieron una enorme repercusión. En el ocaso del siglo XX, la cultura hacker enfrentó otro gran juicio sumarísimo contra uno de sus iconos editoriales. La Motion Picture Association of America y todos los grandes estudios a los que representaba emprendieron en enero de 2000 acciones legales contra el editor de *2600*, Eric Gordon Corley (más conocido como Emmanuel Goldstein), por difundir en su página web y en su edición en papel el DeCSS (Decoder Content Scramblins System), un programa informático que permitía visualizar los DVD bajo el sistema operativo libre GNU/Linux. El caso fue posible gracias a la Digital Millennium Copyright Act (DMCA). La demanda fue interpuesta por la DVD Copy Control Association, participada por la Motion Picture Association of America, la Business Software Alliance y la Electronic Industries Alliance.

Se sabe que el DeCSS fue creado por tres hackers europeos y liberado en octubre de 1999 por el único del que se conoció su identidad, Jon Lech Johansen, un programador noruego de por entonces 16 años, conocido como DVD Jon. Inmediatamente, la Motion Picture Association of America se echó encima y empezó a

demandar a todos los sitios web que almacenaban una copia de DeCSS o publicaban un enlace a un *mirror* con el código. En esa *caza*, llegaron a demandar a decenas de sitios web y personas, entre éstos, el sitio de noticias Slashdot, por simples enlaces en sus informaciones. Muchos de los propietarios de estos sitios sabían que, de llegar a los tribunales, la demanda no prosperaría, pero la mayoría quitó los enlaces para evitar costosos procesos que no podían afrontar. Sin embargo, la revista *2600* mantuvo el enlace en su sitio web. A la vez, la gran industria cinematográfica metió el miedo en el cuerpo a mucha gente e hizo creer a los medios tradicionales —generalmente partidarios de las leyes de propiedad intelectual ligadas a la sociedad industrial— que DeCSS era un programa para piratear los DVD y así justificar una demanda por piratería informática, cuando no era así. Lo que DeCSS hacía era permitir ver películas en GNU/Linux compradas legalmente.

En enero de 2000 saltó la noticia a los medios: Jon Johansen vio registrada su casa y todos sus ordenadores e incluso su teléfono móvil fueron confiscados, sufriendo además un interrogatorio en comisaría de seis a siete horas. El registro fue realizado a instancias de la Motion Picture Association of America, que, sin embargo tuvo dificultades para encontrar argumentos legales con los que acusarle. En Noruega, donde se programó el DeCSS, no es ilegal la ingeniería inversa cuando tenga por objeto la interoperabilidad. El Parlamento noruego tuvo que pedir formalmente disculpas a Johansen por el trato recibido y el Gobierno le concedió el Premio Karoline por su aportación a la sociedad al crear DeCSS. Muy diferente fue la resolución del caso al otro lado del Atlántico.

La Electronic Frontier Foundation se hizo cargo de la defensa de *2600* por mantener el enlace. El problema de fondo que se planteó fue que la Motion Picture Association of America pretendía determinar la manera en que un usuario utiliza un producto, incluso después de haberlo comprado, de manera que el comprador nunca es, de facto, propietario de lo que compra, al considerarse el DVD un software que está obligado a reproducirlo sólo en sistemas propietarios como Windows y MacOS. Además, se coartaba la libertad del usuario mediante un control de códigos regionales, de modo que un DVD comprado en Estados Unidos no se podía reproducir en Europa o Australia, por ejemplo. Esas barreras eran superadas por el DeCSS, que otorgaba libertad al usuario.

La defensa de la revista *2600* insistió en sus alegaciones de que el DeCSS no era un sistema de copia, sino un sistema para poder leer los DVD en cualquier máquina y en cualquier parte del mundo, saltándose los códigos regionales que impedían reproducir los discos de un país en máquinas de otro, y que además otorgaba poder al usuario al permitirle eludir los anuncios bloqueados y programados para ser reproducidos y visualizados sin opción de saltárselos. Además, la defensa de Goldstein, encabezada por Martin Garbus —uno de los más prestigiosos abogados de Estados Unidos en causas relacionadas con la libertad de expresión—, se basó en que prohibir enlazar información constituye una forma de censura, máxime al ser arbitraria, pues *The New York Times* y la CNN, por ejemplo, habían dado a conocer la misma información por la que se condenaba a *2600*. La defensa intentó convencer también al tribunal de que aquel código era expresivo, frente al argumento de la acusación, que lo consideraba meramente funcional. La acusación arguyó que un código informático no es un instrumento de comunicación, sino análogo a una máquina, neutro, y, por tanto, no está protegido por la Primera Enmienda de la Constitución de Estados Unidos que consagra la libertad de expresión. *2600* perdió el caso y la apelación. "Fue un caso sobre el control de la tecnología en sí misma y de no permitir a los consumidores la capacidad de manipular cosas de una manera que les convenga. Esto es lo que realmente molestó a la industria" (Goldstein, 2009: 574).

Aquella fue una de las primeras grandes batallas de la vieja sociedad industrial contra la incipiente cultura colaborativa que hunde sus raíces en la ética hacker:

> Ingeniería inversa, Linux, *cracking*, criptografía, leyes anti-copyright, libertad de expresión y de información, secretos industriales, activismo de red... se mezclan en esta historia de elefantes corporativos entrando en Internet como la cacharrería y una cibersociedad a cada paso más indignada por un conflicto que algunos llaman la «Guerra contra la CDA (Communications Decency Act) II» (Molist, 2000).

Nuevos escenarios se abrieron en la confrontación entre la ética y cultura hackers y el viejo sistema. El caso DeCSS sentó precendente en la batalla de la industria discográfica contra Napster[68], mientras nuevos conceptos como P2P (*peer to*

[68] El Napster original (1999-2001) fue un servicio pionero *peer-to-peer* (de igual a igual) para distribuir y compartir de manera libre en la Red música en formato MP3. Fue tremendamente popular hasta que fue clausurado oficialmente por vulnerar los derechos de autor a consecuencia de las acciones legales emprendidas por la Recording Industry Association of America. Tras su quiebra, por las millonarias indemnizaciones, el nombre «Napster» fue vendido y se utilizó como marca de una nueva tienda de venta de música *online*.

peer), sistemas de intercambio de contenidos como BitTorrent y formatos de audio digital como el MP3 empezaron a abrir brechas entre los nuevos y cada vez más numerosos exploradores de la Red, y los viejos poderes industriales. Por primera vez, se ofrecían herramientas a los consumidores para decidir por sí mismos, para ampliar su capacidad de elección y saltarse el filtro de los canales tradicionales de distribución dominantes (Goldstein, 2009: 581).

El concepto de piratería comercial empezó a difundirse erróneamente asociado a la cultura hacker, contraria a esta práctica, pues en la cultura hacker no se busca el lucro a costa del trabajo ajeno: "No somos partidarios de la piratería de ninguna manera. Las personas que venden los CD que han pirateado están claramente lucrándose de la obra de otra persona. Pero compartir música a través de la Red no es lo mismo" (Goldstein, 2009: 582).

Nuevas herramientas culturales e intelectuales como el software libre, el *copyleft* o el P2P son instrumentos con los que socavar el orden económico y corporativo, pero también el jurídico y político, enfrentándose al poder de los Estados-nación y los monopolios y oligopolios; fomentan nuevos valores sociales y culturales en conflicto con el poder tradicional del viejo capitalismo industrial. En particular, las redes P2P han reconfigurado los flujos de información y datos, pasando de arriba hacia abajo, a una red de pares o iguales, libre y, por lo tanto, han reconfigurando también la arquitectura de la Red. Y además de contenido (audio, vídeo, texto), también permiten compartir valiosos bienes informáticos como el tiempo de procesamiento y el disco duro.

> Los *peer-to-peer* son sistemas distribuidos formados por nodos interconectados capaces de autoorganizarse en topologías de red con el propósito de compartir recursos tales como contenido, ciclos de CPU, almacenamiento y ancho de banda, capaces de adaptarse a las fallas y acomodar poblaciones transitorias de nodos, manteniendo niveles de conectividad y de desempeño aceptables, sin requerir la intermediación o el apoyo de un servidor centralizado o autoridad (Androutsellis-Theotokis y Spinellis, 2004: 337).

El uso de tecnología P2P tiene también, por lo tanto, consecuencias políticas. Jérémie Zimmerman ahonda en ello:

> […] la gente ha tenido un ejemplo práctico [en Napster] de cómo la tecnología P2P descentralizó la arquitectura [de la Red]. De hecho, Napster estaba un poco centralizado en aquella época, pero sembró la idea de una arquitectura descentralizada.

> Todo el mundo tenía un ejemplo concreto que demostraba que la arquitectura descentralizada era buena para la sociedad y, si lo era para compartir cultura, también es bueno para compartir conocimiento. El intercambio de conocimiento es en suma lo fundamental cuando debatimos cómo sortear la censura o cómo erradicar la narración política para construir un sistema democrático y una sociedad mejores (Assange *et al.*, 2012: 81).

Por paradójico que nos parezca ahora, Napster fue precursor del concepto original de Facebook[69], también de iTunes y Spotify (Bruns, 2014: 2651), que probablemente no hubiesen existido sin Napster. Pero, sobre todo, Napster inició la economía colaborativa *peer-to-peer* y se convirtió en una amenaza para la industria y para la propia arquitectura de un sistema oligopolista.

> Lo que siguió a Napster […] no fue un declive terminal de las actividades de intercambio de archivos en línea, como habrían deseado los ejecutivos de la industria del derecho de autor, sino más bien el florecimiento de una amplia gama de plataformas y tecnologías para la difusión de música, películas, software y cualquier otro contenido que pueda servirse en formatos digitales (Bruns, 2014: 2648).

Al igual que sucedió con los hackers, tanto Napster como cualquier plataforma en línea heredera de la filosofía hacker —como las páginas web de The Pirate Bay, Megaupload o Rojadirecta— y sus usuarios han sido criminalizados y acosados judicialmente por la gran industria y la autoridad estatal para poder seguir dictando "cómo, cuándo y dónde se puede acceder al contenido" (Goldstein, 2009: 588), estableciendo sus propios controles y restricciones, y las reglas de juego. Irremediablemente, las comparaciones del modelo Napster con el de WikiLeaks también han aflorado.

> WikiLeaks sólo marca una nueva fase en un cambio permanente en el equilibrio de poder entre los Estados y los ciudadanos, de la misma forma que Napster ayudó a socavar el control de los principales sellos discográficos sobre la industria musical (Bruns, 2014: 2646).

Como hemos visto, los desencuentros de los hackers y de todo cuanto rezume a cultura hacker con la justicia y la autoridad del Estado-nación vienen de largo y han marcado de manera determinante la percepción social del hacker. No en vano, "una de las realidades desafortunadas del mundo hacker ha sido sus encontronazos regulares

[69] Sean Parker, cofundador de Napster, participó en la creación de Facebook y fue su primer presidente. Es, además, miembro del consejo de Spotify.

con diversas formas de aplicación de la ley" (Goldstein, 2009: 179). Sin embargo, se suele decir que el primer gran proceso contra un hacker se inició el 8 de enero de 1990, consideración basada tanto en el impacto mediático que alcanzó, a nivel internacional, como en la sustancialidad de la propia acción y el hecho de que su autor fue el primer ciudadano estadounidense sometido a juicio en Estados Unidos por haber violado la ley federal de 1986 que protege a los sistemas de computación de la acción de los hackers. Su protagonista: Robert Tappan Morris, acusado de propagar en 1988 el primer gusano en la historia de la Red, al que bautizó con su propio nombre y que infectó y colapsó seis mil computadoras —de un total de sesenta mil conectadas en red, por entonces—, entre el 2 y el 3 de noviembre de 1988, fecha que pasó a la historia de la computación como el *Jueves Negro* por el pánico que causó en la NASA, RAND Corporation (Research And Development), el Pentágono, las universidades de Berkeley, Stanford y Princeton, el MIT, el Lawrence Livermore National Laboratory e incluso la red de comunicación militar MILNET (Military Network).

El propósito de Morris no era malicioso. Según confesó, viralizando el gusano pretendía hacerse una idea del tamaño de la Red. Acusado de fraude y abuso de computadora, Morris, por entonces de 24 años de edad, fue declarado culpable de los cargos federales el 22 de enero de 1990. La pena: cuatrocientas horas de servicio comunitario, tres años de libertad condicional y multa de 10.050 dólares. El juicio sentó jurisprudencia al ser la primera vez que se sentaba en el banquillo de los acusados un hacker enjuiciado bajo la Computer Fraud and Abuse Act de 1986.

Este caso dio la vuelta al mundo gracias a la cobertura que le dieron los medios de comunicación de masas, con textos intoxicados por los prejuicios éticos y estéticos y los tópicos que durante la década de 1980 habían ido asentando e inoculando en la población. Baste como ejemplo el artículo publicado en el periódico español *El País* el 15 de noviembre de 1988 titulado 'Robert Tappan Morris', firmado por Albert Montagut, donde la criminalización de la comunidad hacker, los tópicos y algunos desaires son el *leit motiv* de este argumentario contra los hackers:

> Robert Tappan Morris tiene toda la apariencia de un genio. Es feo, lleva unas enormes gafas, el pelo largo y descuidado, y le gustan las corbatas de flores de color fucsia. Su cerebro se transforma cada vez que activa su computadora y los dígitos verdes de su PC iluminan su rostro. Desde hace unos días, el FBI le ha situado en el centro de una investigación que puede ocasionarle serios problemas. Robert es el padre del virus informático que paralizó la red Arpanet, una de las secciones más

> importantes del Departamento de Defensa norteamericano. Es el nuevo rey de los hackers o delincuentes electrónicos.
>
> Robert Tappan Morris es el prototipo de los hackers, nombre con el que se conoce en aquel país a los delincuentes electrónicos, los auténticos creadores de la cultura del software, los infatigables trabajadores sin sueldo que pasan las noches en vela copiando diskets pirateando, comiendo pizza, bebiendo Seven Up sin azúcar e introduciéndose en los hogares ajenos a través de las computadoras. Los hackers comenzaron a formarse clandestinamente, en 1950, en los laboratorios de informática del Massachusetts Institute of Technology (MIT). Robert Tappan Morris es un claro ejemplo de la última generación de estos info-maniacs estadounidenses, locos por invadir los sistemas y redes informáticas del Gobierno con virus destructores y paralizantes (Montagut, 1988).

También los medios alternativos especializados en cultura hacker se hicieron eco de este caso. La revista *2600* publicó un artículo durante el proceso titulado 'Morris found guilty', cuyo tono era, obviamente, antitético al de los medios de masas tradicionales:

> El Gobierno argumentó que Morris escribió intencionalmente el programa gusano para romper las computadoras de «interés federal» que no estaba autorizado a utilizar, y al hacer esto impidió su uso autorizado y causó un mínimo de 1.000 dólares en daños.
>
> Varios miembros del jurado dijeron que era obvio que Morris no tenía intención de hacer daño. Pero dicen que el daño nunca habría sucedido si Morris no hubiese puesto el gusano allí. Ninguno de los miembros del jurado tenía computadora.
>
> Un miembro del jurado dijo de Morris: «Creo en su integridad. No pienso que hubiese ninguna malicia intencionada».
>
> Otro dijo que Morris «no era un criminal. No creo que deba ir a prisión. No creo que la cárcel vaya a hacer nada por él. Para mí la cárcel es para los criminales, y él no es un criminal. Creo que alguien deberá agradecérselo al final».
>
> En su edición del 26 de noviembre de 1988, poco después de que el gusano hiciese su aparición, *The New York Times* describió a Morris como un «fascinado con potentes ordenadores y obsesionado con el universo creado por redes interconectadas de máquinas».
>
> El año pasado, el senador Patrick Leahy de Vermont, dijo: «No podemos obviar que si dejamos experimentar hoy a un inquisidor de 13 años de edad, mañana puede desarrollar las telecomunicaciones o la tecnología informática para llevar a Estados Unidos al siglo XXI». También expresó dudas de que cualquier ley sobre virus informáticos pueda ser eficaz (Goldstein, 2009: 155).

Más clarificadores son los últimos párrafos del artículo publicado en *2600*:

> Sí, lo hizo. Admitió hacerlo. No tenía intención de causar daño, pero cometió un error de programación. El hecho sorprendente es que un error de programación pueda causar tanta confusión. A esto se añade el hecho de que los agujeros de los que hizo uso eran perfectamente conocidos en la comunidad de Internet. Sin embargo, no

> se hizo nada para cerrar los agujeros hasta después de lo sucedido. Parece que alguien debería responder por esta negligencia en sus responsabilidades. Y no nos olvidemos de otro hecho importante: Morris nunca se registró en otro sistema informático sin autorización. No hay ninguna prueba de que alguna vez lo hubiese planeado. Simplemente envió un programa para recopilar datos a través de los canales normales y legales. Eran datos a los que nunca debería haber tenido acceso, pero gracias a los agujeros en el sistema lo hizo.
>
> Morris ha cometido un error. Es parte del juego de aprendizaje por el cual ha sido proscrito. Esta tecnología se encuentra todavía en su infancia y, como cualquier sistema, sus límites necesitan ser evaluados constantemente. Estamos cometiendo un error muy grave si decidimos simplemente centrarnos en los aspectos legales discutibles de lo que hizo, en lugar de aprender de lo que nos ha enseñado.
>
> Somos condenadamente afortunados de que fuese Morris quien lo hizo. Porque si lo hubiese hecho primero alguien malicioso o inmaduro el daño habría sido real (Goldstein, 2009: 156).

Como ya hemos visto, en la cultura hacker nada parece casual y todo cuanto acontece y se sucede tiende a cerrar círculos que completan una narrativa coherente. El autor del primer gusano de la era Internet es hijo de Robert Morris, exjefe científico en el Centro Nacional de Seguridad Informática, división de la Agencia de Seguridad Nacional de Estados Unidos (NSA), hoy en el ojo del huracán y principal objetivo de los hacktivistas por las filtraciones de documentos del caso Snowden que demuestran cómo la NSA se ha convertido en una suerte de Gran Hermano *postorwelliano* y que confirman las sospechas que ya tenía la comunidad hacker en la primera mitad de la década de 1990, cuando ya había una creencia común de que la Agencia de Seguridad Nacional de Estados Unidos estaba supervisando el tráfico en Internet y llamadas telefónicas internacionales.

Ilustración 7: Disquete con el código fuente del gusano creado por Robert Tappan Morris.

Fuente: Intel Free Press en Flickr
https://www.flickr.com/photos/intelfreepress/10483246033

El proceso de Morris tuvo, como otros muchos casos de hackers procesados, un efecto paradójico, pues éste se convirtió en un mito viviente en la comunidad hacker.

Robert Tappan Morris trabaja actualmente como profesor de Ciencias de la Computación en el MIT y en su laboratorio de Inteligencia Artificial. Un disquete que contiene el código de su virus se exhibe en el Computer History Museum de Mountain View (California).

Al igual que veremos en el caso de Julian Assange y de su organización WikiLeaks, los de Morris y todos los hackers auténticos procesados por la justicia no han hecho más que constatar que "cualquier ley creada para «eliminar» el *hacking* simplemente no va a funcionar" porque "está en la naturaleza" del hacker jugar y experimentar con computadoras (Goldstein, 2009: 210).

La verdad no conoce fronteras. La información necesita ser libre. La tecnología es la clave.

—Peter Gabriel.

II. HACKTIVISMO

II.1. DEL HACKERISMO AL HACKTIVISMO

Desde su misma germinación, en la cultura hacker se halla una inmanencia política que cuestiona el modelo y convenciones sociales, la organización del trabajo, la gestión estatal y corporativa de la información y los datos, y la privatización y comercialización del conocimiento. Sin embargo, esa inmanencia política ha trascendido y se ha manifestado en distintos grados y maneras en diferentes épocas y en distintas generaciones de hackers. Desde el misantropismo de las primeras generaciones de hackers, hasta la exhibición pública del gregarismo de las nuevas generaciones de hacktivistas, observamos que en sus acciones —ya sean sólo para escribir nuevo software libre para beneficio de la comunidad o por pura diversión, o para introducirse en los sistemas de la autoridad para revelar sus secretos o cuestionar su seguridad— prevalece un espíritu libertario de defensa de la libre expresión e información y una apología de la voluntad y poder del individuo frente a la abúlica masa alienada. Sin embargo, ese espíritu libertario es por primera vez puesto al servicio de la defensa activa de los derechos humanos a partir de la segunda mitad de la década de 1990, cuando una vanguardia de hackers pasa a la acción política directa y nace el hacktivismo. Como veremos en este capítulo, los hacktivistas no han perdido ni la curiosidad ni el entusiasmo ni la pasión que caracterizan al hacker, pero en su actividad prevalece su abnegación en la defensa pública de las libertades del individuo, un sacrificio trascendente que parece disipar la diversión inherente.

Hacktivismo es un neologismo que une activismo (sociopolítico) y *hacking* (computacional). Aunque se ha difundido, principalmente por Wikipedia, que el crítico cultural y autor Jason Sack fue quien usó por primera vez este término en un artículo publicado en *InfoNation*, en 1995, dedicado a la artista multimedia taiwanesa Shu Lea

Cheang, el grupo hacker Cult of the Dead Cow siempre ha reivindicado para sí la invención de este vocablo. De hecho, el término *hacktivismo* fue acuñado en 1994 por uno de los miembros de Cult of the Dead Cow conocido como Omega, para describir el hacking con propósitos políticos y vinculado a la defensa de derechos humanos (Ruffin, 2004).

> El origen de la palabra «hacktivismo» se remonta a Omega, un viejo miembro de cDc, que empezó a usarla como un juego para describir las acciones de protesta en línea. Oxblood (Ministro de Exteriores de cDc y creador del subgrupo Hacktivismo) se apropió de la palabra y empezó a usarla en serio; después lo hicieron muchos periodistas (Cult of the Dead Cow, 2001)[70].

El hacker canadiense Oxblood Ruffin se afanó en ofrecer una definición sustantiva del hacktivismo que lo protegiese de un contagio semántico del concepto *ciberguerra* que Arquilla y Ronfeldt habían empezado a trazar para RAND Corporation. Y llegó a una definición temprana para la palabra *hacktivismo*: "el uso de la tecnología para mejorar los derechos humanos a través de medios electrónicos" (Ruffin, 2004).

Count Zero —otro miembro de Cult of the Dead Cow— amplió esta definición del hacktivismo en 1999, vinculando explícitamente la defensa de los derechos humanos con el flujo libre de información:

> [Hacktivismo es] centrarse en dar poder a las personas… con las herramientas del hacktivismo… haciendo que el mundo conozca las injusticias y abusos contra los derechos humanos… en otras palabras, conseguir que el flujo de información estalle en todo el mundo… sin obstáculos y sin censura… Eso es el hacktivismo (Jordan y Taylor, 2004: 98)

Desde la eclosión del hacktivismo en la esfera pública, en el año 1998, la literatura sobre el activismo hacker se ha extendido por campos como la sociología, el derecho, la filosofía, los estudios y análisis de seguridad o los estudios culturales, pero ha sido escasamente abordado en las teorías de la comunicación y la información. Samuel (2004: 23) identifica dos tendencias en el abordaje del hacktivismo, ambas nutridas de informes de incidentes, cobertura en prensa y declaraciones en línea de los propios hacktivistas: una que mira al hacktivismo en el contexto de la seguridad informática, la guerra de información y el ciberterrorismo, desarrollada principalmente

[70] Todas las citas a Cult of the Dead Cow son traducciones propias de los texos originales, en inglés.

en los trabajos de Dorothy Denning (2001) y, sobre todo, de los analistas de RAND David Ronfeldt y John Arquilla (1993, 1999, 2001), que han influido notablemente en aproximaciones tan recientes como la de Jarvis, Macdonald y Chen (2015), y otra tendencia que mira al hacktivismo en el contexto de la desobediencia civil y de los medios de comunicación, descrita principalmente por Wray (1998, 1999), Manion y Goodrum (2000), Vegh (2003) y Tim Jordan y Paul Taylor (1999, 2002, 2004).

La aproximación sociológica y política de Jordan y Taylor ubica el hacktivismo en el punto de intersección entre el *hacking*, los tiempos virales y las nuevas manifestaciones de protesta y resistencia globales, por lo que sólo puede ser plenamente entendido en el contexto tanto de su patrimonio y herencia hackers como de las nuevas respuestas políticas innovadoras a las redes de comunicación de las sociedades virales (Jordan y Taylor, 2004: 2, 145, 164). De hecho, al utilizar "técnicas informáticas tomadas de la comunidad hacker preexistente", Jordan y Taylor consideran que "es difícil identificar definitivamente dónde termina el *hacking* y dónde comienza el hacktivismo" (2004: 2).

Estos dos autores identifican el hacktivismo como el "intento de solución al problema de llevar a cabo de manera efectiva la protesta política contra un sistema que está expandiendo su alcance global en cada vez más formas inmateriales" (Jordan y Taylor, 2004: 30). Más concretamente, en Jordan y Taylor "los hacktivistas son el matrimonio entre el espíritu del *hack* y el espíritu de protesta en el contexto de los tiempos virales" (2004: 39).

Manion y Goodrum (2004: 14) definen el hacktivismo como "el (a veces) uso clandestino del *hacking* computacional para ayudar a promover causas políticas". A este enfoque proactivo del hacktivismo añaden también prácticas reactivas comunes entre los hacktivistas, principalmente:

> […] arremeter contra el dominio corporativo de las telecomunicaciones y de los medios de comunicación, la rápida expansión de la *datavigilancia*[71] y la hegemónica intrusión de la «cultura de consumo» en la vida privada de los ciudadanos comunes" (Manion y Goodrum 2000: 14)[72].

[71] La *datavigilancia* es la vigilancia sistemática de los registros electrónicos de las actividades de cualquier persona (teléfonos móviles, correo electrónico, uso de tarjetas de crédito, etc.).
[72] Todas las citas tomadas de Manion y Goodrum fueron traducidas del texto original, en inglés, por el autor de esta tesis.

Las motivaciones políticas del hacktivismo también son revisadas por Vegh (2003), quien coincide con Wray y Jordan y Taylor en identificar dos categorías de hacktivistas: los activistas clásicos que se han informatizado y los hackers que han pasado a la acción política.

El hacktivismo huye del estigma criminal y se autorreafirma como forma legítima de protesta y desacato al poder autoritario en el ciberespacio. Manion y Goodrum coinciden con Wray (1998, 1999) en ofrecer una evaluación del hacktivismo como nueva expresión de desobediencia civil. Estos autores caracterizan a los hacktivistas como una nueva generación hacker "claramente motivada por el avance de las preocupaciones éticas y que cree que sus acciones deben ser consideradas actos legítimos de desobediencia civil (electrónica)" (Mannion y Goodrum, 2000: 16), en los que se fusionan "la conciencia social del activista político y el talento del hacker informático" (p. 18), y cuyo objetivo puede ser "cualquier individuo, corporación o nación que se considere que es responsable de la opresión de los derechos éticos, sociales o políticos de otros" (p. 14).

Huschle (2002), sin embargo, es reticente a incluir todas las manifestaciones hacktivistas en el marco de la desobediencia civil, pues entiende que, a diferencia de los activistas tradicionales, la clandestinidad en la que se suelen mover algunos hacktivistas y su transgresión de límites legales anima a los medios de comunicación, gobiernos y sistemas legales a mantener la etiqueta de "terrorismo electrónico" sobre acciones legítimas de desobediencia civil electrónica.

El hacktivismo se asienta en una ideología cooperativa y liberal para la consecución de la justicia social, la descentralización del poder, la transparencia política y la libertad de información, a la vez que busca contrarrestar la tendencia mercantilista de Internet como mercado electrónico global dominado por corporaciones capitalistas transnacionales que se han convertido en "las fuerzas políticas más poderosas de nuestra época" (Klein, 2001: 393), donde reside el poder. Por lo tanto, el hacktivismo representa una amenaza potencial para el viejo capitalismo industrial y su gestión de la propiedad intelectual, y también para los gobiernos nacionales y sus niveles de seguridad (Manion y Goodrum, 2000: 14). Frente a la *generosidad* del Estado-nación, los hackers proponen la cooperación —el *peer to peer*, de igual a igual— como herramienta para alimentar el desarrollo de la sociedad. A la

presunta liberalidad del Estado de Bienestar —que no es tal, pues el servicio social se cobra en impuestos mediante un sistema coercitivo y punitivo— se le contrapone la cooperación voluntaria como resultado de la suma de fuerzas que hace avanzar a todos los individuos que participan y a los colectivos, comunidades o sociedades que éstos integran. Esa visión ha sido adoptada en los últimos tiempos por las ONG, que han pasado de una estrategia de la caridad heredada del Estado-nación a otra de la cooperación táctica (dirigida a individuos, colectivos, comunidades o sociedades) y cooperación estratégica (entre las propias organizaciones no gubernamentales, organizadas en red).

Meyer y Thomas identifican un *ethos* antisistema que proporciona unidad ideológica para la acción colectiva. Los hackers, dicen, "han sabido utilizar sus habilidades colectivas en represalia por actos contra la cultura que perciben como injustos"; estas acciones son una manifestación de resistencia promovida por la ética hacker, "un *ethos* compartido de oposición a lo que perciben como una dominación *orwelliana* de una elite que controla la información" (Meyer y Thomas, 1990: 23-24).

Es precisamente el control de la información lo que genera los nuevos conflictos sociopolíticos en el ciberespacio.

II.2. LAS GUERRAS DE LA INFORMACIÓN EN LA RED

La acción reivindicativa de carácter sociopolítico es lo que define al activismo. La canalización de esa acción hacia el ciberespacio por vías computacionales y mediante técnicas de *hacking* permite nuevas formas de acción y protesta políticas que desafían las estrcturas autoritarias y las normas que las sustentan, configurando nuevos movimientos sociales virtuales que se oponen a la expansión de la inclinación capitalista por convertir todo en mercancía, también (en) Internet, y que promueven el acceso libre a la información creando herramientas para la lucha por mantener el ciberespacio fuera del control corporativo y estatal (Jordan y Taylor, 2004: 164).

Alexandra Whitney Samuel describe una variedad de acciones hacktivistas que incluye desfiguraciones de páginas web, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sentadas y sabotajes virtuales, y desarrollo de software. Se trata de un "uso no violento de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos" (Samuel: 2004: iii).

El conflicto de los activistas del ciberespacio con el Estado-nación y las corporaciones ha sido dramatizado con una nueva terminología bélica para una nueva realidad: las guerras en red (*netwars*) y las ciberguerras (*cyberwars*). Estos nuevos términos han contribuido a articular toda una teoría sobre *infoguerras* para los tiempos ciberespaciales, en las que la lucha se libra con alta tecnología pensada y desarrollada por las mentes más brillantes de nuestros tiempos: científicos computacionales, programadores, matemáticos, físicos, ingenieros de redes y expertos en minería y análisis de grandes bases de datos; la elite intelectual del siglo XXI (Elías, 2015a). La superioridad ahora la da el dominio de la información. La batalla se libra por controlar su recopilación, almacenamiento, procesado, comunicación y presentación, o por controlar que no existan esos controles.

> La revolución de la información implica el surgimiento de un modo de guerra en la que ni la masa ni la movilidad decidirán los resultados; en cambio, el bando que sepa más, que pueda dispersar la niebla de la guerra y envolver a un adversario, gozará de ventajas decisivas (Arquilla y Ronfeldt, 1993)[73].

[73] Cita del *abstract* de *Cyberwar is Coming!*, publicado por RAND Corporation. Disponible en: <http://www.rand.org/pubs/reprints/RP223.html> (último acceso: 3 de febrero de 2015). Todas las demás citas de este texto incluyen los números de página del libro *In Athena's Camp: Preparing for Conflict in the Information Age* —editado por Arquilla y Ronfeldt y publicado por RAND Corporation en 1997—, que contiene este artículo en el Capítulo 2. Todas las citas de las obras de estos autores fueron traducidas de los originales, en inglés, por el autor de esta tesis.

Arquilla y Ronfeldt fueron los primeros en acuñar los términos *netwar* y *cyberwar*, diferenciando entre los conflictos sociales librados en Internet y las ciberguerras militares. Definen las guerras en red como conflictos relacionados con la información a gran escala —suelen ser transfronterizas— entre naciones o sociedades, de manera que podemos encontrar guerras en red entre Estados-nación rivales o entre gobiernos y actores no estatales que pueden estar o no asociados a las naciones y, en algunos casos, organizados en grandes coaliciones transnacionales. Las *netwars* se alimentan del desarrollo de nuevas tecnologías que favorecen y refuerzan las organizaciones en red, instantáneas, ubicuas y flexibles. Este tipo de conflicto tiene extensiones políticas, económicas y sociales, además de algunas formas militares de guerra, siempre dirigidas a las comunicaciones y a la información. Su objetivo es alterar o dañar lo que una población objetivo sabe o piensa que sabe de sí misma y el mundo que la rodea, afectando a la opinión pública, a la de una elite o a ambas, mediante la diplomacia, la propaganda y campañas psicológicas, la subversión política y cultural, el engaño o la interferencia en medios locales, la infiltración en redes informáticas y bases de datos o esfuerzos para promover la disidencia o movimientos de oposición a través de redes informáticas.

Las *netwars* no son exclusivas del ciberespacio y suelen desarrollarse tanto en la realidad física como en la virtual siguiendo una estrategia descentralizada ejecutada por nodos dispersos (los nodos pueden ser sociedades, organizaciones, grupos o individuos con intereses compartidos —lícitos o ilícitos— y que pueden actuar en público o en privado). Las guerras en red no son, por lo tanto, guerras reales, en su definición tradicional, pero sí pueden ser instrumentos para evitarlas.

Por el contrario, las operaciones militares son inherentes a las ciberguerras. El objetivo es controlar, interrumpir o destruir sistemas de información y comunicaciones. Para lograrlo, es necesario saber todo sobre el adversario y evitar que éste sepa mucho sobre nosotros, inclinando la balanza de la información y el conocimiento a favor de uno. De esta manera, se pueden evitar además grandes inversiones de capital y trabajo en operaciones militares clásicas.

Vegh (2003) define la ciberguerra como ciberataques asociados al Estado. Arquilla y Ronfeldt (1993), por su parte, enumeran distintas aplicaciones para la ciberguerra mediante el uso de diversas tecnologías de comunicación e información,

en particular para mando y control, inteligencia, transformación y distribución, comunicaciones tácticas, posicionamiento, identificación amigo-enemigo, sistemas de armas *inteligentes* o intrusiones y alteraciones de los circuitos de información y comunicación del adversario, entre otras.

Las *infoguerras* —ya sean *netwars* o *cyberwars*— han constatado la importancia del control sobre la información como herramienta de poder en los tiempos virales como nunca antes. Aunque Aquilla y Ronfeldt encuentran antecedentes históricos a las ciberguerras. Para éstos, los mongoles son un ejemplo clásico de una fuerza ancestral que luchó según principios de ciberguerra, organizándose más en red que jerárquicamente. También las fuerzas combinadas de Vietnam del Norte y el Viet Cong —una fuerza militar menor que derrotó a una gran potencia moderna— operaron más como red que como institución. En estos casos, los oponentes derrotados de los mongoles y de los vietnamitas eran grandes instituciones diseñadas para una guerra tradicional ensayada. Por ello, consideran que las instituciones pueden ser derrotadas por redes, que las redes pueden ser tomadas para hacer frente a las redes enemigas y que, en definitiva, el futuro puede pertenecer a quien domine la forma de la red por la que circula la información (Arquilla y Ronfeldt, 1993: 34-40)

Las guerras de la información canalizan un *poder blando* que se contrapone al *poder duro*: la batalla por la inteligencia *vs* la aplicación de la fuerza bruta del enfrentamiento militar o económico; *noopolitk vs realpolitik* (Arquilla y Ronfeldt, 1999). El término *noopolitik* (*nu-oh-poh-li-teek*) fue acuñado por estos dos autores para catalogar una forma emergente del arte de gobernar que hace hincapié en la importancia de compartir globalmente ideas y valores —a través del ejercicio del *poder sutil* persuasivo en lugar del *poder duro* militar tradicional—, que contrasta con el abordaje tradicional y los enfoques realistas y neorrealistas, en términos de promoción del Estado en la arena internacional mediante la negociación, fuerza o uso potencial de la fuerza.

Este nuevo enfoque estratégico se basa en "la manipulación de información, diferente a la antigua política de equilibrios nacionales de poder" Castells (2001: 159), de manera que el poder se conquista y se conserva no por la fuerza bruta, sino por la fuerza del conocimiento.

> […] el mundo se está moviendo hacia un nuevo sistema en el que «poder» se entiende principalmente en términos de conocimiento, y la estrategia informacional debe centrarse en el «equilibrio del conocimiento», a diferencia del «equilibrio de fuerza» (Arquilla y Ronfeldt, 1999: 43-44).

Noopolítica toma su raíz de *noos*, o *noûs*, que Aristóteles designa como la parte más alta del alma, el intelecto, el *noûs* como conocimiento intelectual e inmediato de las esencias de las cosas, ahora aplicado a la estrategia política como *poder blando*.

> Mientras que la *realpolitik* a menudo apunta a la coacción mediante el ejercicio del poder duro (cuya esencia es militar), la *noopolitik* pretende atraer, convencer, incorporar e imponer con poder blando (cuya esencia es no militar). Aceptando que la raíz *noos* se refiere a la mente, noopolitik significa tener una capacidad sistemática para llevar a cabo interacciones exteriores en términos relacionados con el conocimiento. Para ello se requiere estrategia de información, de hecho […] noopolitik es estrategia de información (Arquilla y Ronfeldt, 1999: 40-41).

Mauricio Lazzarato (2006) profundiza en la *noopolitik* como conjunto de nuevas técnicas de control que se ejerce sobre el cerebro, implicando a la atención, para controlar la memoria y su potencia virtual, siendo la modulación de la memoria la función más importante de la noopolítica. De esta manera, una nueva política a distancia establece nuevas relaciones de poder que toman como objeto la memoria y su *conatus*, la atención. Este nuevo tipo de poder, que ha experimentado un desarrollo sin precedentes gracias a la computación y la telemática, y a la emergencia de los medios de comunicación electrónicos, no es homologable al de la disciplina ni al del biopoder, ya que no se ejerce ni sobre los cuerpos ni sobre las poblaciones, sino sobre el cerebro de los sujetos configurados como públicos. Pero estos tres dispositivos diferentes de poder no se sustituyen unos por otros, sino que se integran para vertebrar la sociedad de control.

> Si las disciplinas moldeaban los cuerpos constituyendo hábitos principalmente en la memoria corporal, las sociedades de control modulan los cerebros y constituyen hábitos principalmente en la memoria espiritual. Existe entonces un moldeado de los cuerpos, asegurado por las disciplinas (prisiones, escuela, fábrica, etcétera), la gestión de la vida organizada por el biopoder (Estado de Bienestar, políticas de la salud, etcétera) y la modulación de la memoria y de sus potencias virtuales regulada por la noo-política (redes hertzianas, audiovisuales, telemáticas y constitución de la opinión pública, de la percepción y de la inteligencia colectivas). Sociológicamente tendríamos esta secuencia: la clase obrera (como una de las modalidades de encierro), la población, los públicos. El conjunto de estos dispositivos, y no sólo el último, constituye la sociedad de control (Lazzarato, 2006: 100)

Por lo tanto, el nuevo enfoque político no liquida, sino que complementa al de la *realpolitik*:

> La noopolitik contrasta con la realpolitik, la postura tradicional de fomento del poder estatal en la escena internacional, por medio de la negociación, la fuerza o el uso potencial de la fuerza. La realpolitik no desaparece en la era de la información, pero permanece centrada en el Estado en una era que está organizada en torno a redes, incluidas las redes de estados. En un mundo que se caracteriza por la interdependencia global, configurado por la información y la tecnología, la capacidad para responder a los flujos de información y a los mensajes transmitidos por los medios se convierte en herramienta esencial para fomentar una determinada agenda política (Castells, 2001: 183).

La *noopolitik* emerge como la respuesta política al desarrollo del ciberespacio, la infoesfera[74] y la noosfera (*noosphere*)[75] —este último, un entorno global de información que incluye el ciberespacio y todos los demás sistemas de información, incluidos los medios de comunicación—, y al surgimiento de una nueva doctrina de la seguridad para la era de la Sociedad Red. El nuevo enfoque exige una estrategia de flujos de información adaptable a un entorno global que abarque todos los aspectos de esta dimensión, desde los tecnológicos hasta los conceptuales, y dirigidos a un espacio subjetivo en la mente de los individuos, cuya suma es la sociedad, la cual se estimula por las corrientes informativas.

Arquilla y Ronfeldt (1999: 35) identifican cinco tendencias que hacen cada vez más viable la noopolítica: la creciente estructura de interconexión global, el continuo fortalecimiento de la sociedad civil global, el aumento del *poder blando*, la nueva importancia de las ventajas cooperativas frente a las comparativas o competitivas, y la formación de la noosfera global.

La noosfera global también posibilita la intervención de los movimientos sociales y de las ONG, influyendo en las mentes de personas de todo el mundo al intervenir en la noosfera, es decir, en el sistema de comunicación y representación donde se forman las categorías y donde se construyen los modelos de comportamiento (Castells, 2001: 183).

---

[74] Mientras que el ciberespacio hace referencia fundamentalmente a la información que fluye por la Red, el infoespacio incluye ésta y la que circula en los medios masivos tradicionales (prensa, radio, televisión).

[75] El concepto de noosfera fue acuñado por el científico ruso Vladimir Ivanovich Vernadsky (1863-1945), para quien la emergencia de la cognición humana transforma la biosfera. El jesuita y filósofo francés Pierre Teilhard de Chardin (1881-1955) tomó el concepto y explicó la noosfera como el lugar donde ocurren todos los fenómenos del pensamiento y la inteligencia, una atmósfera cognitiva que conecta a todos los seres humanos.

De esta forma, pasamos de una concepción estatocéntrica de la *realpolitik* que sólo reconoce selectivamente y con reticencias a ciertos actores no estatales, y que funciona mejor cuando los Estados descartan totalmente el sistema global, a otra no estatocéntrica en la que los actores no estatales —principalmente del mundo del comercio y de la sociedad civil— están actuando en red y globalmente, ganando fuerza y remodelando el ambiente mundial gracias a interconexiones transnacionales cada vez más complejas (Arquilla y Ronfeldt, 1999: 30).

La noosfera constituye, por lo tanto, el ambiente idóneo para el desarrollo del ciberactivismo y, en particular, para el hacktivismo, que encuentra en las redes de comunicación electrónicas el instrumento útil para distribuir globalmente un *poder blando* —contrapoder al del Estado-nación— y viralizar una visión alternativa del mundo que reconfiguren la opinión pública y agendas políticas.

> […] el espectacular abaratamiento de la transmisión de información ha abierto el campo a organizaciones en red vagamente estructuradas e incluso a individuos. Estas organizaciones no gubernamentales y redes son particularmente eficaces para penetrar Estados sin tener en cuenta las fronteras y usando grupos nacionales para obligar a los líderes políticos a centrarse en sus agendas preferidas. La revolución de la información ha aumentado enormemente el número de canales de contacto entre sociedades, una de nuestras tres dimensiones de la interdependencia compleja[76] (Keohane y Nye 1998: 83-84).

Para Keohane y Nye (1998: 94), el *poder blando* descansa en última instancia en la credibilidad, la cual deriva principalmente de la producción y difusión de información (pública) libre. En base a los incentivos para crearla, identifican tres tipos diferentes de información que son fuentes de poder: 1) la información gratuita, a cargo de actores que están dispuestos a crearla y distribuirla a cambio de una compensación que no es económica, sino de reputación; 2) la información comercial, realizada por gente dispuesta a crearla y enviarla por un precio económico, y 3) la información estratégica, tan vieja como el espionaje, que confiere gran ventaja a los actores sólo si sus competidores no la poseen (Keohane y Nye 1998: 84-85).

[76] La interdependencia compleja tiene tres características principales: 1) canales múltiples conectan las sociedades y fomentan relaciones interestatales (canales normales supuestos por los realistas), transgubernamentales (se flexibiliza el supuesto realista de que los Estados actúan coherentemente como unidades) y transnacionales (se flexibiliza el supuesto de que los Estados son las únicas unidades); 2) la agenda de las relaciones interestatales consiste en múltiples temas que no están colocados en una jerarquía clara o sólida, de manera que la seguridad militar no domina consistentemente la agenda, y 3) la fuerza militar no es empleada por los gobiernos contra otros gobiernos de la región cuando predomina la interdependencia compleja (Keohane y Nye, 1998).

> La capacidad de difundir información gratuita aumenta el potencial para la persuasión en la política mundial. […] Si un actor puede persuadir a los demás a adoptar valores y políticas similares, el poder duro y la información estratégica pueden llegar a ser menos importantes. El poder blando y la información gratuita pueden, si son lo suficientemente persuasivos, cambiar las percepciones del propio interés y, por lo tanto, alterar la forma en cómo se utilizan el poder duro y la información estratégica. Si los gobiernos o las ONG quieren sacar ventaja de la revolución de la información, tendrán que conseguir reputación para tener credibilidad […] (Keohane y Nye 1998: 94).

Sin embargo, estos autores rebajan el optimismo en el *poder blando* canalizado en la noosfera, ya que entienden que "la revolución de la información no ha causado cambios dramáticos en las otras dos condiciones de interdependencia compleja" (Keohane y Nye 1998: 84). Lo cierto es que la fuerza militar sigue desempeñando un papel fundamental en las relaciones entre los Estados y, en situaciones de crisis, la seguridad aún supera a otras cuestiones de política exterior, como sucedió tras los ataques del 11 de septiembre de 2001 en Estados Unidos, que derivaron en una *cruzada* en Oriente de este país y sus aliados, con frentes de guerra abiertos en Irak o Afganistán. El problema radica en que la información está fluyendo por espacios ocupados y controlados por los Estados.

> Una de las razones por las que la revolución de la información no ha transformado la política mundial en una nueva política de la interdependencia compleja completa es que la información no fluye en el vacío, sino en un espacio político que ya está ocupado. Otra es que […] en muchas áreas, los supuestos realistas sobre el predominio de las cuestiones de fuerza y seguridad militares siguen siendo válidos. Durante los últimos cuatro siglos, los Estados han establecido la estructura política dentro de la cual fluye la información a través de fronteras (Keohane y Nye, 1998: 84).

Julian Assange va un paso más allá. El fundador de WikiLeaks denuncia la existencia de un *poder duro* en el ciberespacio, su militarización mediante el control de las redes de comunicación por las fuerzas y cuerpos de seguridad del Estado. Para Assange, el ciberespacio, que "originalmente se planteó como un espacio civil, ha sido militarizado, se ha convertido en un espacio militarizado" por los Estados-nación, "en el sentido de una ocupación militar", con el fin de interceptar cualquier comunicación a través de cualquier dispositivo conectado a la Red e imponer "una ley marcial en lo que respecta a nuestras comunicaciones; simplemente no podemos ver los tanques, pero están" (Assange *et al.*, 2012: 33). Pero a diferencia del *poder duro* físico, que castiga al cuerpo y a la propiedad física e inflinge dolor físico y moral, esta nueva

dimensión virtual del *poder duro* ataca a la intimidad del individuo sin causarle dolor. Así, la sobreexposición en la Red de la vida privada del individuo y de sus opiniones no supone riesgo físico alguno, pero sí un gran riesgo para su libertad, ya que las vierte en un espacio *militarizado* sin percibir la amenaza ni las consecuencias:

> […] usamos [Internet] para comunicarnos entre nosotros, con nuestras familias, revelando lo más íntimo de nuestras vidas. Así que, de hecho, nuestras vidas privadas han entrado en una zona militarizada. Es como tener un soldado debajo de la cama. Es una militarización de la vida civil (Assange *et al.*, 2012: 33).

Existe, por lo tanto, una nueva dimensión del *poder duro* institucional en el ciberespacio —disimulado como *poder blando*— para controlar los mecanismos de formación del consenso y facilitar un nuevo modelo de totalitarismo cognitivo, cuya capacidad de control y coerción se considera más eficaz que el de la fuerza bruta física. Esta "reubicación del conflicto en el terreno de las redes de comunicaciones supone efectivamente una redefinición de la guerra moderna", pero también "una redefinición de las propias redes de comunicaciones" por el uso de estas como objetivos militares (Almirón Roig, 2007).

II.3. DESOBEDIENCIA CIVIL ELECTRÓNICA

Las reflexiones teóricas sobre conflictos emergentes y potenciales en el ciberespacio han sido el paso previo necesario para la ejecución de nuevas estrategias tanto militares como de contestación civil. La conceptualización de las infoguerras por parte de actores estatales y su teorización para elaborar una nueva doctrina militar han originado toda una corriente de pensamiento y han sido respondidas en la misma forma por actores no estatales que han asentado las bases teóricas para una nueva forma de desobediencia civil que se desarrolla en el ciberespacio. Wray (1998, 1999) sitúa las primeras teorizaciones y advertencias de la autoridad en los primeros análisis sobre guerras de información en red de Arquilla y Ronfeldt para RAND Corporation, uno de los principales laboratorios de ideas (*think tank*) del mundo, encargado de la formación de las Fuerzas Armadas de Estados Unidos.

> A pesar de algunas intervenciones radicales y de los intentos de replantear las formas dominantes de la teoría de la guerra de información militar y de inteligencia, la mayor parte del material, como es lógico, es producido según los gustos de RAND, la Universidad Nacional de Defensa, el Departamento de Defensa, la Fuerza Aérea de Estados Unidos o iniciativas del sector privado. El meme[77] de la guerra de información parece haber sido extendido y promulgado en gran medida por paranoicos de la seguridad de redes y otros interesados en conservar la propiedad digital. Pero hay señales de que la guerra de información se está extendiendo a otras áreas (Wray, 1998)[78].

A los planteamientos de Arquilla y Ronfeldt —cuyo enfoque es puramente militar—, Wray responde con un enfoque de las infoguerras que atiende a la contraparte civil. Wray (1998) —cofundador y teórico del Electronic Disturbance Theater— observa que los modelos dominantes de infoguerra, principalmente teorizados por los analistas de RAND, han acaparado mayor atención que los enfoques

[77] El término *meme* fue acuñado por Richard Dawkins en su libro *El gen egoísta* (1976) y aparece definido en el diccionario Merriam-Webster como "idea, comportamiento, moda o uso que se extiende de persona a persona dentro de una cultura". Por otra parte, la palabra *meme* se emplea cada vez más para referirse a cualquier imagen o texto, a menudo de contenido humorístico, que se comparte viralmente en las redes sociales durante un periodo breve (Fundeu: http://www.fundeu.es/recomendacion/meme-termino-valido/). El profesor José Luis Orihuela ofrece una explicación más detellada: "Los memes son ideas originales, útiles o divertidas, cuyo atractivo hace que la gente las adopte y comparta con otros. La Red se ha convertido en un entorno especialmente apto para la difusión de estas *ideas infecciosas*, que han encontrado en la blogosfera su medio ambiente natural. Un meme puede ser desde un broma hasta un negocio, pasando por una aplicación útil, un proyecto comunitario, una leyenda urbana, un concurso o un juego. La capacidad *memética* de la blogosfera se está utilizando de manera creciente para impulsar estrategias de *marketing viral*, en las que la idea de base circula no sólo por su atractivo (Gmail), sino también por su intencionada promoción (FON)". En http://www.ecuaderno.com/2006/02/16/memes-los-virus-de-la-mente/ (último acceso: 20 de junio de 2014).

[78] Todas las citas tomadas de Wray (1998, 1999) son traducciones propias del texto original, en inglés.

dirigidos al uso estratégico de la información por parte de actores no estatales. Por ello, anima a abordar con cautela el concepto de infoguerra dominante de Aquilla y Ronfeldt —"[…] es necesario identificar con qué intereses se promulgan esas ideas", advierte Wray en Paquin (1998)[79]— y a redefinir desde el activismo electrónico la doctrina de la infoguerra adoptada por gobiernos y difundida por medios de comunicación.

> Lo que nosotros podemos llamar un ejemplo de «hacktivismo» los teóricos de la guerra de información lo definen peyorativamente como una subcategoría de ciberterrorismo (Wray, en Paquin, 1998).

Mientras Arquilla y Ronfeldt (1993) arguyen, desde su visión estatocéntrica, que la información se ha convertido en "un recurso estratégico que puede resultar tan valioso e influyente en la era postindustrial como el capital y el trabajo lo han sido en la era industrial", Wray (1998) traslada el análisis a la potencialidad del uso de información estratégica por parte de movimientos civiles y establece cinco categorías de hacktivismo o, más ampliamente para Wray, de política extraparlamentaria de acción directa en la Red: activismo informatizado, infoguerra de base, desobediencia civil electrónica, *hacking* político y resistencia a la guerra futura. Se trata de la primera propuesta para una taxonomía del hacktivismo.

[79] Todas las citas tomadas de Paquin son traducciones propias del texto original, en inglés.

II.4. TAXONOMÍA DEL HACKTIVISMO

Una de las mayores preocupaciones de los estudiosos del activismo hacker ha sido ofrecer una taxonomía del hacktivismo, conforme a la elasticidad de las ideas y acciones identificadas en éste, que permita una mejor aproximación epistemológica a su complejidad.

II.4.1. Primeras propuestas teóricas

Wray (1998, 1999) es el primero en proponer cinco categorías para el hacktivismo, en las que profundizamos a continuación.

II.4.1.1. Actvismo informatizado

El activismo informatizado existe en las intersecciones de los movimientos político-sociales y la comunicación mediada por ordenador (Wray, 1998). Sus primeras expresiones se remontan a mediados de la década de 1980, cuando activistas y organizaciones no gubernamentales empezaron a usar redes informáticas independientes y progresistas para una comunicación transfronteriza relativamente fácil y rápida (Wray, 1998; Murphy, 2000a).

> Estas redes fueron fundadas por individuos con experiencia en el área de la comunicación y en la colaboración internacional dentro del mundo de las ONG, con un profundo compromiso para poner las nuevas técnicas de comunicación a disposición de los movimientos que trabajaban a favor del cambio social. La mayoría de estas redes fueron fundadas por un número reducido de personas que dedicaron sus equipos personales y todo su tiempo libre a difundir la comunicación electrónica entre sus colegas que trabajan a favor del cambio (APC, 2001).

Las primeras manifestaciones de activismo informatizado y en red se dieron gracias a la financiación del proyecto Interdoc por parte del International Development Research Centre de Canadá. El proyecto se concretó en el Acuerdo Valletri, firmado en el año 1984 por un grupo de organizaciones no gubernamentales de Europa, América, Asia y África, que se comprometieron a utilizar líneas telefónicas internacionales para enlazar sus equipos informáticos y cooperar entre ellas de manera

más eficaz[80]. Fue así como se constituyó la primera red computacional transnacional para los movimientos sociales (Murphy, 2001).

En sus inicios, varios miembros de Interdoc utilizaron el servicio de *email* de una red comercial de correo europea llamada GeoNet, con base en Alemania. Un grupo de activistas por la paz y el medio ambiente de Londres había llegado en 1985 a un acuerdo con GeoNet para operar una subred sin fines de lucro denominada GreenNet y trabajaron para que otros activistas y organizaciones civiles compartiesen el mismo sistema para poder comunicarse de manera más fluida y en red. En 1987, GreenNet obtuvo sus propios equipos y comenzó a operar independientemente de GeoNet.

A la par, otros pioneros del activismo informatizado fundaron en 1985 PeaceNet, una red de activistas por la paz creada en Estados Unidos como proyecto de la Foundation for the Arts of Peace, con la cooperación de cuatro organizaciones: Community Data Processing, Center for Innovative Diplomacy, Ark Foundation y la propia Foundation for the Arts of Peace. Un año después, PeaceNet integró la red ecologista EcoNet, creada por el Farralones Institute, en Estados Unidos; una fusión que se concretaría en 1987 en la creación del Institute for Global Communications. Ese mismo año, los activistas de GreenNet empezaron a colaborar con sus contrapartes de PeaceNet/EcoNet mediante el uso de comunicaciones electrónicas.

A finales de 1989, varias redes en Suecia (NordNet), Canadá (Web Networks), Brasil (IBASE), Nicaragua (Nicarao/CRIES) y Australia (Pegasus) ya estaban intercambiando información entre sí prácticamente en tiempo real y a distancia, al igual que con el Institute for Global Communications y GreenNet. En primavera de 1990, estas siete organizaciones fundaron la Association for Progressive Communications con el fin de proveer de infraestructuras, herramientas y destrezas para el uso de tecnologías de la comunicación y de la información a grupos e individuos movilizados por la paz, los derechos humanos, la justicia social y la protección del medio ambiente.

[80] Los firmantes del Acuerdo Valletri en 1984 fueron: International Documentation Centre (Italia) —fundado por la ONU—, International Development Education Research Agency (Canadá), Instituto Brasileiro de Analises Sociais e Economicas (Brasil), International Coalition for Development Action (Béligica), CODESRIA (Senegal), Asia Monitor Research Centre (Hong Kong), Antenna (Holanda), SATIS (Holanda), Human Rights Information and Documentation Systems (Noruega), Instituto Latinamericano de Estudios Transnacionales (Chile) y DESCO (Perú).

En junio de 1995, la Association for Progressive Communications obtuvo estatus consultivo general ante el Consejo Económico y Social de Naciones Unidas, pero su colaboración con este órgano supraestatal ya había comenzado en 1989, en las preparaciones de la Conferencia de Naciones Unidas sobre Medio Ambiente y Desarrollo, más conocidas como Cumbre de la Tierra, que tuvo lugar en Río de Janeiro (Brasil) en 1992. Como la Association for Progressive Communications poseía la única red de comunicaciones internacional dedicada a la sociedad civil que existía por entonces, la secretaría del Foro de Naciones Unidas utilizó sus canales. No había otra manera para ellos de distribuir información de manera tan económica y eficaz (la ONU comenzó a distribuir por su propia cuenta información en la Red varios años después). En 1992, la Association for Progressive Communications creó el primer centro de comunicaciones electrónicas para las ONG y delegados de Naciones Unidas que participaron en la Cumbre de la Tierra de Río. En septiembre de aquel año, más de 17.000 usuarios de 94 países utilizaban estas redes.

Aquella red virtual, global y progresista de activistas empezó a funcionar cuando Internet, tal y como la conocemos hoy, ni siquiera existía.

> La mayoría de los *hosts* utilizados por las redes de activistas eran sistemas autónomos y no había protocolos de uso común para automatizar el intercambio de datos y la distribución de correo electrónico entre los usuarios. Muchos de los proveedores incluso tenían «portales humanos»: personas que copiaban y pegaban mensajes manualmente entre su red y una red de otro país. A finales de la década de 1980, los técnicos (frecuentemente autodidactas) tenían que viajar de una parte a otra del mundo, para instalar el software y crear el código de programas, de manera que los sistemas de computación de diferentes ONG pudiesen «hablarse» y por lo tanto enviar correo electrónico y compartir información (Murphy, 2000b).

La primera gran experiencia internauta, en su sentido estricto, para los activistas tuvo lugar en la Cumbre Mundial de la ONU sobre Desarrollo Social, celebrada en Copenhague en 1995. NordNet —organización sueca adscrita a la Association for Progressive Communications— guió a un grupo de activistas de comunicaciones de Dinamarca en la instalación de comunicaciones electrónicas para esta cumbre. Fue la primera vez que se dispuso de navegadores web y que el público pudo acceder a un sitio web de la Association for Progressive Communications.

El proceso de informatización y globalización del activismo tradicional se desarrolló paralelamente a una cada vez mayor concienciación política en la

comunidad hacker. Pero sus caminos no se encontraron hasta la segunda mitad de la década de 1990, con Internet como herramienta facilitadora y las infoguerras como la primera puerta al ciberactivismo.

II.4.1.2. Infoguerra de base

La conceptualización de la infoguerra surge de la necesidad de elaborar una nueva doctrina militar ante las emergencias de un nuevo escenario geopolítico tras la caída del Muro de Berlín y del nuevo espacio cíber y sin fronteras. Wray (1998) se remonta a principios de la década de 1990 para encontrar los orígenes de esta nueva doctrina militar. La caída del Telón de Acero, la disolución de la Unión Soviética y el consecuente ocaso de la retórica de la Guerra Fría como racionalización de la intervención extranjera; las nuevas guerras *inteligentes* y televisadas —seguidas por el gran público casi en tiempo real, como la de Irak— y el auge del ciberespacio hicieron que el aparato militar de Estados Unidos y sus centros de inteligencia, junto con sus aliados en sectores corporativos y financieros, viesen necesario elaborar una nueva doctrina militar. "Su respuesta fue la guerra de información y la amenaza *infoterrorista*" (Wray, 1998).

Wray describe lo que denomina "infoguerra de base" como una intensificación del activismo informatizado. Su aportación es el contrapunto al enfoque militarista de las infoguerras. Para Wray, la distinción principal entre las formas anteriores de activismo informatizado y las formas de guerra informacional de base está en el grado de intensidad, el deseo de incitar a la acción y la capacidad para hacerlo a una escala global. Se trata de una guerra de palabras —una guerra de propaganda— que supone un primer paso para alejarse de la idea de Internet como simple espacio para la comunicación y el comienzo para transformar las palabras en hechos, en acciones directas. Más que un mero intercambio de información y de diálogo, lo que hay es un deseo de empujar las palabras a la acción, de usar medios alternativos en Internet como vehículos para incitar a la acción, en lugar de simplemente describir o informar.

Stefan Wray elucida que los actores de las infoguerras de base que emergen son plenamente conscientes de que están en un escenario global que les ofrece el don de la ubicuidad, capacidad de inmediatez y sentido de interconexión global.

A la clásica centralidad y jerarquía de la palabra dogmática del Estado-nación —*Dei Verbum*— se le opone ahora una nueva palabra performativa que surge del diálogo horizontal entre actores no estatales, que se distribuye por canales alternativos que compiten en el mismo espacio comunicativo —la Red— con los canales de información de la autoridad, que se confronta con el discurso oficial y lo desafía, que es generadora de ideas, argumentos y acciones, y que se configura como contrapoder.

II.4.1.3. De la desobediencia civil electrónica a la desobediencia civil híbrida

La desobediencia civil electrónica es la tercera categoría en la que se manejan los movimientos civiles de resistencia en la Red. Es heredera de la desobediencia civil tradicional, descrita por Manion y Goodrum (2000: 15) como una técnica de resistencia y protesta, cuyo propósito es lograr un cambio social o político dirigiendo la atención de la gente a determinados problemas e influyendo en la opinión pública. La desobediencia civil implica una ruptura pacífica de leyes que se consideran injustas; no tolera actos violentos o destructivos proyectados y sistematizados, y se centra en exponer injusticias y despertar conciencias. Es la misma visión aportada por Honderich (1995) sobre la desobediencia civil como un llamamiento moral a la acción, un ejercicio de coerción persuasiva —no violenta, aunque conlleva la amenaza de la violencia incidental— y una negativa a seguir en el cumplimiento de leyes y normas que se consideran injustas.

La incorporación de las tecnologías digitales de la información y la comunicación a estos movimientos de resistencia y su ocupación de *espacios* en Internet han permitido a los activistas ampliar y potenciar su capacidad de organización, comunicación, publicación y acción directa (Manion y Goodrum 2000: 15). Esta nueva forma de acción es descrita por Stefan Wray (1998, 1999) como desobediencia civil electrónica. A la vez que se expande en el ciberespacio, la desobediencia civil electrónica interactúa con la realidad física, dando lugar a lo que Wray (1998) denomina desobediencia civil híbrida: la conjunción de acciones de desobediencia electrónica y las tradicionales formas de desobediencia civil en las calles. Wray esclarece que mientras las segundas se han caracterizado principalmente por las sentadas, bloqueos y ocupaciones físicos, la desobediencia civil electrónica se ha caracterizado en sus primeras manifestaciones por la estrategia de los bloqueos,

sentadas[81] y ocupaciones virtuales como formas de acción electrónica directa, masiva y descentralizada.

El pensamiento de Wray sobre la desobediencia civil está inspirado por la crítica a la autoridad del Estado de Henry David Thoreau en *La desobediencia civil* (1948) y por su aforismo "el mejor gobierno es el que menos gobierna".

> […] desde la publicación de *La desobediencia civil* de Thoreau hemos visto aplicadas en diversos grados tácticas individuales, de grupo y de desobediencia civil masiva por un buen número de movimientos sociales en Estados Unidos. En la segunda mitad del siglo XX, la desobediencia civil se ha practicado en cada década. A veces ha sido un éxito. Otras veces ha fracasado. Teniendo en cuenta que no es probable que las realidades objetivas de la sociedad estadounidense alteren radicalmente el corto plazo, podemos asumir con seguridad que los movimientos sociales radicales, de una forma u otra, van a continuar adoptando las estrategias y tácticas de desobediencia civil en el siglo XXI (Wray, 1999).

Wray toma la idea de la desobediencia civil electrónica del libro *Electronic Civil Disobedience & Other Unpopular Ideas* (1996), del colectivo Critical Art Ensemble, formado por artistas, activistas y teóricos. La obra se publicó como secuela de otra anterior publicada en 1994 con el título *The Electronic Disturbance*. Ambas sostienen que en la era del capital global, nómada, líquido, disperso y electrónico, es necesario asentar las bases para el crecimiento de una resistencia también móvil, líquida y ubicua, diseminada en las redes electrónicas. Critical Art Ensemble sostiene la emergencia de idear nuevas formas digitales y electrónicas de actvismo, ante la pérdida de eficacia de las formas clásicas de desobediencia civil. La única manera de enfrentarse al capital en su forma electrónica móvil actual es ejecutar la resistencia en el mismo lugar donde se concentra ahora el capital: el ciberespacio.

Las raíces intelectuales de Critical Art Ensemble, especialmente en sus concepciones nómadas del capital y de la resistencia, se hunden en la obra de Hakim Bey (1991) *T. A. Z. The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*, que a su vez se nutre de las ideas sobre la nomadología de Gilles Deleuze y Felix Guattari (1987) en *A Thousand Plateaus*. Bey nos habla de la creación de zonas

[81] Una sentada virtual consiste en una acción consensuada por una multitud de usuarios de la Red ejecutada desde diferentes lugares y distintos horarios sobre un sitio web, con el objetivo de ralentizar su servicio, llegando en ocasiones a saturar el sitio. La primera *netstrike* conocida se realizó en 1995, en protesta por las pruebas nucleares francesas en el atolón de Mururoa. Luego, esta estrategia se trasladó a América y se hizo conocida mundialmente con The Electronic Disturbance Theatre y Ricardo Domínguez. Una netstrike es una acción simbólica y conceptual, una forma artística e inteligente de respuesta social, utilizando medios electrónicos (Molist Ferrer: 2014).

autónomas temporales y nómadas en la Red que se constituyen en plataformas en las que se activa y desde las que se lanza la desobediencia civil electrónica. El movimiento de información a través de las diversas ciber-redes de resistencia se ha dicho que se ha producido rizomáticamente[82], moviéndose horizontalmente, de forma no lineal y por subterráneos (Wray, 1999).

Sin embargo, Wray (1998, 1999) apela a una desobediencia civil híbrida que implica múltiples tácticas, fruto de la combinación de acciones en las calles y acciones en el ciberespacio. La rebelión zapatista es considerada la primera manifestación de infoguerra de base en red y de desobediencia civil híbrida. Los zapatistas de México contaron con el apoyo de una comunidad internacional de seguidores que rápidamente abrió un frente de batalla en Internet. Esta experiencia prozapatista global en la Red provocó un cuestionamiento o replanteamiento de las construcciones teóricas de RAND, pero desde una perspectiva de base más radical liderada por Harry Cleaver, profesor de la Universidad de Texas en Austin y persona clave en el Proyecto Chiapas, un servicio de distribución de información por correo electrónico. Wray (1998) caracteriza la experiencia zapatista en la década de 1990 como una guerra de palabras, más que como un conflicto militar prolongado.

> Académicos, activistas y periodistas, tanto de la izquierda como de la derecha, han dicho que los zapatistas deben su supervivencia […] en gran parte a una guerra de palabras. Esta guerra de palabras, en parte, es la guerra de propaganda desatada con éxito por líderes zapatistas como el Subcomandante Marcos y por simpatizantes no zapatistas en todo México y en el mundo. Tal propaganda y retórica ha sido, por supuesto, transmitida a través de los medios de comunicación de masas más tradicionales […]. Pero un componente importante de esta guerra de palabras ha tenido lugar en Internet. El 1 de enero de 1994 hubo una explosión de la presencia zapatista en Internet a través de listas de correo electrónico, grupos de noticias, listas de discusión y sitios web (Wray, 1998).

La reacción civil a la matanza de Acteal, en Chiapas (México), el 22 de diciembre de 1997, es un claro ejemplo del poder de la Red para la desobediencia civil híbrida. En aquella masacre, cuarenta y cinco indígenas tzotziles fueron asesinados por paramilitares contrarios al Ejército Zapatista de Liberación Nacional. Los activistas vincularon a los paramilitares con el Partido Revolucionario Institucional (PRI), que gobernó México durante setenta y un años seguidos. Dieciséis niños, niñas y

[82] "Rizoma es una palabra tomada de la botánica que se utiliza para describir ciertos tipos de tubérculos que, como un sistema de raíces, se expanden horizontal y subterráneamente" (Wray, 1999).

adolescentes, veinte mujeres y nueve hombres fueron asesinados mientras oraban en una iglesia. La noticia sobre la matanza se extendió rápidamente a través de las redes globales de Internet prozapatistas. En cuestión de días hubo protestas y acciones en los consulados y embajadas de México en todo el mundo. Hasta 1998, la desobediencia civil electrónica se había mantenido como una reflexión teórica; la masacre de Acteal fue un punto de inflexión en la actitud de los activistas hacia la infraestructura de Internet, vista a partir de entonces como una herramienta para la comunicación y como un espacio para la acción directa. Se inició un cambio hacia una posición más híbrida que abrió nuevas posibilidades para el activismo político en red (Wray, 1998).

La desobediencia civil electrónica es la primera transgresión, a la que siguen el *hacking* político y la resistencia a la guerra futura. Cada manifestación y éxito de estas tres transgresiones nos demuestra lo lejos que estamos del ideal de Internet como espacio de libertad y nos acerca más a un "territorio en conflicto al borde de una zona de guerra" (Wray, 1998).

II.4.1.4. *Hacking* político activo

Wray (1999) vaticinó cambios radicales en las formas de desobediencia civil y un aumento notable de los actores ciberactivistas por el creciente uso de computadoras entre los activistas clásicos, pero también por lo que este autor identifica como politización (activa) de los hackers —que nosotros observamos como *emergencia* política hacker—, convirtiendo el ciberespacio en el escenario principal para la desobediencia civil y para la aparición de nuevos movimientos sociales que se expresan en ciberacciones cada más sofisticadas.

Taylor (2004), al igual que Vegh (2003), ve en el hacktivismo la convergencia de hackers informáticos cada vez más concienciados políticamente y activistas tecnológicamente más habilidosos. Para estos autores, los orígenes diferentes de unos y otros han dado lugar a dos tendencias o tácticas distintas en el hacktivismo: la primera, los hackeos web y de computadoras, y la segunda, los actos de desobediencia civil electrónica, como sentadas virtuales, por ejemplo.

Juris constata en la organización de protestas y actos de desobediencia civil en línea una intención de utilizar "las herramientas de las redes y las lógicas del

capitalismo global contemporáneo para desafiar al propio capitalismo global", en la que los hackers activistas juegan un papel clave "combinando y recombinando códigos culturales —en este caso, significantes políticos—, compartiendo información sobre proyectos, movilizaciones, estrategias y tácticas a través de las redes globales de comunicación" (Juris, 2008: 2, 14).

Para Castells, los hackers políticamente activos se han convertido en un "elemento clave del movimiento por la justicia global" y su capacidad tecnológica los ha situado "en la primera línea del movimiento, liberando al activismo de las limitaciones impuestas a su expresión independiente por el control empresarial de las redes de comunicación" (Castells, 2009: 450).

Sin embargo, todas estas aportaciones teóricas desatienden la irrupción de un nuevo enfoque hacktivista que establece como objetivo prioritario la incursión en el hermético sistema nervioso del poder para extraer y hacer pública la información que circula por éste, al *viejo* estilo hacker pero con nuevos enfoques, estrategias y objetivos adaptados a la nueva realidad. Esta nueva tendencia, que WikiLeaks empezó a liderar desde el año 2006, pero que ya antes habían iniciado los promotores de Cryptome[83], busca propalar los secretos del Estado-nación y de las corporaciones empresariales. Como los hackers de la década de 1980 y primera mitad de 1990, los hacktivistas del siglo XXI entienden que la única manera de mejorar el sistema es introduciéndose en él, descubrir sus procedimientos y fallas, y compartir esos hallazgos haciéndolos públicos[84].

Observamos, además, que una diferencia sustancial entre los activistas tradicionales que han saltado al ciberespacio y los activistas hackers es que los segundos, a diferencia de los primeros, pueden actuar tanto colectiva como individualmente, y lo hacen generalmente en el anonimato o bajo seudónimos que les identifican en su comunidad. Esa naturaleza anónima del hacker activista contrasta con la exposición pública de los rostros e identidades registradas en los archivos civiles, incluso de las trayectorias vitales de los activistas tradicionales. Si éstos entienden que

[83] Cryptome es una fundación privada sin ánimo de lucro, con sede en Nueva York, creada en 1996 por los arquitectos John Young y Deborah Natsios, y soportada por su firma, Natsios-Young Architects. Su misión es publicar en su página web documentos sensibles para gobiernos y corporaciones y crear una librería de acceso libre. El 2 de enero de 2016 contabilizaba 100.200 archivos en 42 gigabytes. Sitio web: https://cryptome.org/ (último acceso: 18 de enero de 2016).

[84] Véase el Capítulo IV, página 287, sobre WikiLeaks.

la transparencia de su *yo* es necesaria para obtener credibilidad, los hackers activistas consideran que preservando su privacidad y anonimato están no sólo protegiéndose de la autoridad, sino además siendo coherentes con sus exigencias para una nueva sociedad que emerja en el ciberespacio y en la que el individuo sería efectivamente libre mediante el anonimato emancipador[85].

Diferencias también sustanciales emergen entre los hacktivistas de la década de 1990 y los hackers de la de 1980. Principalmente,

> los hackers siguen obsesionados con la inmersión en el abstracto entorno del código de computación, mientras que los hacktivistas conectan esta inmaterialidad a la importancia de una razón social o política, incluso cuando una acción está coordinada en el ciberespacio o es sobre el ciberespacio (Jordan y Taylor 2004: 35).

Además, según Stallman, nunca hubo un movimiento hacker:

> No se trata de un movimiento, sino de un gusto. Si tienes el gusto de la inteligencia juguetona, si yo hago algo que demuestra esa inteligencia, te gustará verlo y también desearás lograr tales cosas para enseñárselas a los demás. Es más o menos un tipo de arte (Richard Stallman, en Quian, 2013c).

Sin embargo, el hacktivismo sí se configura como movimiento, como una corriente que interviene directamente en la escena política con unos principios. Pero, sobre todo, la diferencia más sustancial entre los primeros hackers y los hacktivistas es que los segundos ya no se mueven sólo por utopías, sino también contra distopías materializadas o en vías de materializarse.

Son principalmente los *cypherpunks* —los ciberlibertarios más radicales— quienes a principios de la década de 1990 teorizan, reflexionan, debaten e informan sobre un modelo utópico de sociedad libre gestada en la Red, cuyas formas primigenias empiezan a experimentar en los subterráneos del ciberespacio y cuya conceptualización y experimentación surge como respuesta a la distopía *orwelliana* que parece estar configurándose en la superficie: una sociedad de control, vigilancia y censura. A las teorías de los *cypherpunks* se suman a mediados de esta década las aportaciones de una nueva generación de activistas que asumen algunos principios de la ética hacker y las contribuciones de hackers que aplican sus ideas y destrezas al activismo político.

[85] Véase IV.6.3.1. Anonymous: el anonimato emancipador, página 387.

Wray (1998) habla del activismo hacker como un "*hacking* politizado" que nosotros observamos más precisamente como *hacking* político activo. El objeto o sujeto *politizado* lo es por ser trascendido por un contenido o conciencia política de origen externo. Sin embargo, el *hacking* computacional guarda un uso ético de la tecnología que trasciende políticamente en su misma ejecución. En el caso de los hacktivistas —los hackers *politizados* para Wray—, Jordan (2002) esclarece que estos intentan aplicar sus habilidades informáticas a una agenda política ya establecida. Es cierto que esa agenda política no había existido entre los primeros hackers informáticos, que habían priorizado la dimensión lúdica del *hacking* como principal pilar ético de su actividad, manteniendo en apariencia la dimensión política en un segundo plano (Torvalds y Diamond, 2001).

Pero la dimensión política del *hacking* emerge una y otra vez en cualquier manifestación y materialización de la defensa de una ética del trabajo apasionado y voluntario y del acceso libre y universal al código, esto es, a la información y al conocimiento. Linux, por ejemplo, es un proyecto gestado por el hacker finlandés Linus Torvalds siguiendo estos principios hackers (Raymond, 1999; Moody, 2001), pero su realización, propalación, defensa y uso extendido afecta políticamente a las sociedades en las que se promueve esta alternativa —"probablemente […] la que ha llevado más lejos la idea de la accesibilidad y el código abierto" (Himanen, 2001: 64)—, ya que permite "pensar en la aplicación del modelo abierto en otras áreas de la vida además de la programación de software" (Himanen, 2001: 53).

Si la información es poder, la información es política *per se*. Y "en la era de la información, la nueva información se crea de manera más efectiva si se permiten prácticas lúdicas y la posibilidad de trabajar a un ritmo personal", de igual modo que "el modelo de libre acceso no solamente se halla justificado desde un punto de vista ético, sino que en la práctica resulta muy potente", hasta tal punto que la propia comunidad hacker, en el Jargon File, lo considera "un bien extraordinario" (Himanen, 2001: 53).

El profesor Johan Söderberg, de la Göteborgs Universitet, aporta luz sobre las ramificaciones políticas del *hacking*:

> Por ejemplo, los hackers que de ninguna manera se consideran a sí mismos «políticos» tienden sin embargo a oponerse a las patentes de software y a la vigilancia estatal de Internet, por citar sólo dos ejemplos. De hecho, estos puntos de vista son tan

> ampliamente compartidos en el *underground* informático que se ven más como fruto del sentido común que de una postura política. Algunos temas, como las campañas contra la expansión de las leyes de propiedad intelectual y la defensa de la libertad de expresión, han sido agregados a agendas políticas y son promovidos activamente por grupos de presión hackers; dos ejemplos son la Free Software Foundation y la Electronic Frontier Foundation. Estas organizaciones están claramente involucradas en política, aunque sostienen que estos intereses cortan por ejes diferentes de los de la división derecha-izquierda tradicional (Söderberg, 2009: 89-90).

Las interpretaciones políticas tanto de la ética hacker como de la retórica sobre la libertad de expresión e información, y la privacidad del individuo en el ciberespacio, han sido heterogéneas, desde las afinidades encontradas con el liberalismo clásico (Coleman y Golub, 2008; Fuchs, 2014) o las más extensas lecturas libertarias y anarquistas (Meyer y Thomas, 1990; Sterling, 1992; Anderson, 1993; May, 1994; Rosteck, 1994; Moglen, 1999; Thierer y Szoka, 2009; Jurgenson y Rey, 2014), pasando por las explicaciones contradictorias de la espaciosa izquierda europea tradicional, en la que existen dos corrientes principales: la que cree que "el movimiento hacker podría revitalizar las viejas luchas de la izquierda, no sólo por la libertad individual, sino también en contra de la injusticia y la desigualdad", y otra corriente dominante que expresa una "sospecha profundamente arraigada […] hacia la tecnología informática y, por extensión, a sus más celosos usuarios, es decir, los hackers" (Söderberg, 2009: 90).

Esta desconfianza hacia la tecnología digital y el escepticismo sobre su poder emancipador predicado por los hackers arraiga en la lectura política que un grueso de la izquierda ha hecho de los orígenes de Internet, de su primigenia forma, ARPAnet, vinculada al aparato militar estadounidense, y del desarrollo desde la época de la Guerra Fría de aplicaciones militares de alta tecnología para la vigilancia y el control globales. Similares perspectivas opuestas se hallan también en lo que Thierer y Szoka (2009) identifican como ciberlibertarismo, corriente en la que encontramos pesimistas que describen un ciberespacio controlado y regulado por el Estado que sofoca la libertad de los individuos, y optimistas convencidos de que las herramientas y métodos para evitar la regulación del ciberespacio, la censura y el control triunfarán finalmente. Thierer y Szoka examinan el ciberlibertarismo como una de las dos ideologías opuestas que emergen en el discurso político contemporáneo sobre la libertad y el control de la información en el ciberespacio; la otra es el cibercolectivismo. Mientras

la primera se centra en minimizar la regulación gubernamental tanto en el plano social como en el económico —entrelazados para los ciberlibertarios—, la segunda sostiene que Internet debe ser regulado para que se cumpla la amorfa voluntad o interés generales.

> En términos generales, el lema del ciberlibertario es «Vive y deja vivir» y «¡Manos Fuera de Internet!». El ciberlibertario aspira a minimizar el alcance de la coerción del Estado en la solución de problemas sociales y económicos, y busca en su lugar soluciones voluntarias y acuerdos basados en el consentimiento mutuo (Thierer y Szoka, 2009).

Tecnologías como el software libre y de código abierto y proyectos colaborativos no propietarios como Wikipedia no están, para estos autores, en desacuerdo con el ciberlibertarismo, pero el ciberlibertario considera que la autoridad no debe tomar partido para inclinar el equilibro en una dirección u otra en los debates "abierto *vs* cerrado" y "propietario *vs* no propietario". En lugar de tratar de definir o imponer una única visión utópica, el ciberlibertario busca posibilitar una utopía de utopías, un marco dentro del cual pueden florecer muchos modelos diferentes de organización del comercio y de la comunidad juntos y en competencia unos con otros (Thierer y Szoka, 2009).

Sin embargo, el cibercolectivismo aboga por la regulación estatal o por parte de una elite que guíe a los individuos en sus ciberdecisiones. Aunque Thierer y Szoka observan influencias lejanas de Platón, Rousseau y Marx en la retórica cibercolectivista, atribuyen a esta corriente distintas sensibilidades que van desde posicionamientos de izquierdas "más centrados en las preocupaciones sociales que las económicas" y que consideran que "los recursos digitales deben ser compartidos", hasta otros de derechas que "se centran en controlar el impacto de Internet en la cultura o en la seguridad" (Thierer y Szoka, 2009). En todo caso, desligan a la izquierda cibercolectivista de motivaciones marxistas y de cualquier afán de nacionalización de los recursos digitales, e identifican a sus actores como una suerte de cibersocialdemócratas en un sentido europeo, concediendo un papel generoso a la ley y a la regulación en los asuntos del ciberespacio.

En esta elasticidad en la interpretación de las esencias políticas de la ética hacker y de la retórica de la libre información en el ciberespacio parece emerger un

consenso cada vez mayor en identificar esencias anarquistas —anarcomunistas en algunos casos, anarcocapitalistas en otros— en las exigencias de libertad, emancipación, descentralización y antiautoritarismo. Jurgenson y Rey, por ejemplo, estiman pertinente agregar una tercera categoría a las aportadas por Thierer y Szoka: el ciberanarquismo, que considera la Web como "una herramienta para debilitar o disolver instituciones problemáticas o innecesarias" (Jurgenson y Rey, 2014: 2656). En esa corriente sitúan a WikiLeaks.

Antes de diseccionar el ciberanarquismo, Jurgenson y Rey nos remiten al ciberlibertarismo como "una ideología política consolidada que tiene sus raíces en la cultura hacker en los orígenes de Internet y en el libertarismo estadounidense" (2014: 2656). De la primera ha heredado su oposición a cualquier forma de regulación, censura o cualquier barrera en la Red; del segundo ha tomado la creencia de que las asociaciones voluntarias de individuos son más efectivas en la promoción de la libertad que la intervención del gobierno. A partir de aquí, estos autores establecen sutiles diferencias entre ciberlibertarismo y ciberanarquismo.

> El anarquismo tiene por objeto la abolición de la jerarquía. Como los libertarios, los anarquistas muestran un tremendo escepticismo hacia el gobierno, sobre todo hacia el derecho exclusivo de los gobiernos a utilizar la fuerza contra otros actores. Sin embargo, mientras los libertarios tienden a centrarse en el mercado como un mecanismo para gratificar logros individuales, los anarquistas tienden a verlo como un medio para perpetuar la desigualdad. De este modo, los ciberanarquistas tienden a estar en contra de la consolidación de una infraestructura de Internet privada y de las interferencias del gobierno (Jurgenson y Rey 2014: 2657).

La necesidad de la existencia o no de unas jerarquías meritocráticas parece, por lo tanto, la frontera más definida que separa a los ciberlibertarios de los ciberanarquistas.

El gran consenso que encontramos en las lecturas políticas sobre la ética hacker es que en ésta reside una conciencia política antiautoritaria (Meyer y Thomas, 1990; Sterling, 1992; Raymond, 2001; Himanen, 2001; Goldstein, 2009). En el propio Jargon File se reconoce que en la cultura hacker "hay un fuerte contingente libertario que rechaza la política convencional de izquierda-derecha" y que "la única generalización segura es que los hackers tienden a ser bastante antiautoritarios" (The on-line hacker Jargon File, version 4.4.7, 29 de diciembre de 2003).

Esta actitud contra el poder autoritario ya se intuye en los primeros hackers del Massachusetts Institute of Technology, como Peter Samson, Bob Saunders o Alan Kotok, quienes intentaron usar los primeros ordenadores IBM, de tarjetas perforadas, sin permiso de la *casta sacerdotal* que los hacía funcionar y que los guardaba y protegía con reglas creadas *ex profeso* para impedir el acceso de aquellos primeros hackers y así dificultarles el conocimiento de su funcionamiento. "La regla más rígida de todas era que nadie podía tocar o manipular la propia máquina" (Levy 1984: 27). Para muchos de aquellos primeros exploradores —los hackers originales de Levy—, aquel proceso de aprendizaje fue como una "guerra de guerrillas" contra el *sacerdocio* de la información (Sterling, 1992). Ya en la década de 1980, las nuevas generaciones de hackers empezaron a ligar el código fuente y el software libre con el flujo libre de información y el acceso al conocimiento. Luego, en la década de 1990, los *cypherpunks* enfatizaron la dimensión política del *hacking* con la encriptación.

Podemos con todo esto concluir que la dimensión política de la ética y de la cultura hackers emana en su "intento de refundir, reapropiarse y reconstruir la relación poder-conocimiento que domina cada vez más la ideología y las acciones de la sociedad" (Meyer y Thomas, 1990: 2). Negar la sustancia política de la ética hacker refuerza, por un lado, el discurso penalizador del hacker como mero delincuente sin ideales y, por otro, justifica y posibilita la estrategia destinada a fagocitar —o *civilizar*— a algunos de los más habilidosos miembros de esta comunidad como programadores dúctiles, microsiervos del Estado-nación y de las corporaciones tecnológicas que comercializan hardware y software privativos. Por último, la vieja retórica de criminalización del hacker como potencial terrorista —agudizada con la emergencia hacktivista— evidencia también las connotaciones políticas del *hacking*.

II.4.1.4.1. Software libre para la soberanía del individuo

Junto con los sistemas de encriptación, el software libre se ha convertido en el asunto central de la retórica ciberlibertaria. Si la encriptación es fundamental para garantizar nuestra privacidad y seguridad, el software libre lo es para asegurar el bien común y evitar la privatización del conocimiento, de manera que ambos convergen en un mismo fin: la libertad de información, el acceso libre al conocimiento y la soberanía del individuo.

Para Stallman, "con el software libre los usuarios tienen el control sobre el programa", mientras que "con el software privativo es el programa el que tiene el control sobre los usuarios", de modo que "la lucha por el uso de software libre también es fundamental para la democracia", pero no sólo para garantizar la libertad del individuo, sino también para que cada Estado pueda "recuperar su soberanía informática cambiando el software privativo por el software libre" (Richard Stallman, en Quian, 2013c). Stallman advierte de que el software privativo se ha convertido en una poderosa herramienta de control sobre los Estados, en manos de grandes corporaciones empresariales:

> El asunto es que con el software privativo el programa tiene el control del usuario y el dueño del programa ejerce el poder sobre éste. Y si el usuario es un Estado, el dueño del programa ejerce el poder sobre el Estado. Por eso el Estado tiene que dejar de usar programas privativos (Richard Stallman, en Quian, 2013c).

Una de las lecturas más disruptivas de la dimensión política del *hacking* y del software libre la aporta Eben Moglen, autor del *dotCommunist Manifesto*:

> Existe un mito, como la mayoría de los mitos parcialmente fundados en la realidad, de que todos los programadores informáticos son libertarios. Los de derechas son capitalistas, devotos de sus acciones en bolsa que desdeñan los impuestos, los sindicatos y las leyes de derechos civiles; los de izquierdas odian el mercado y a todos los gobiernos, creen en la encriptación robusta sin importar cuánto terrorismo nuclear pueda causar, y no les gusta Bill Gates porque es rico. Hay, sin duda, base para esta creencia. Pero la diferencia más significativa entre el pensamiento político dentro de la elite digital y fuera de ésta es que en la sociedad red el anarquismo (o más propiamente, el individualismo antiposesivo) es una filosofía política viable (Moglen, 1999)[86].

Moglen (2003b) idealiza un mundo en el que el anarquismo en el desarrollo de software como servicio público reemplazará a la comercialización capitalista del software como mercancía, lo cual dará como resultado un modo más eficiente de organizar la producción intelectual humana y una nueva estructura social.

El *copyleft* —como antítesis del *copyright* y de la aplicación de patentes— sería lo más cercano a ese ideal anarquista. La producción de software ejecutable sin relaciones inherentes de propiedad desarrollaría un software superior, no de forma inmediata pero sí a largo plazo (Moglen, 2003b). Este triunfo del anarquismo como

[86] Todas las citas tomadas de Moglen (1999, 2003a y 2003b) son traducciones propias de los textos originales, en inglés.

modo de producción se manifiesta, en concreto, en la Licencia Pública General GNU de la Free Software Foundation —implementación específica del concepto general de *copyleft*—, cuyo uso de las reglas de propiedad intelectual sólo pretende crear un bien común en el ciberespacio (Moglen, 1999). Un bien común que se protege a sí mismo:

> La apropiación [de software] se puede dar de forma ilimitada siempre que cada modificación de los materiales en el bien común se devuelva en forma de bien común. Cualquier persona que haga un uso no comunitario del bien común está infringiendo la licencia (Moglen, 2003b).

En el desarrollo de software libre existe, por lo tanto, una dimensión política inapelable, una nueva economía política facilitada por la Licencia Pública General GNU, que "ha conseguido crear el mayor y más extenso programa de intercambio de conocimientos del mundo y sin coste alguno" (Moglen, 2003b). El software libre es la materialización del princio en el que se debe sustentar cualquier sociedad emancipada y soberana: el flujo libre de información, un "espectro" que "está acechando al capitalismo multinacional" (Moglen, 2003a).

En el *dotCommunist Manifesto* (Moglen, 2003a) clarifica con gran lucidez la emergencia de la producción y distribución anarcocomunista, que compite con el sistema de propiedades y privaciones capitalista. Moglen reconoce la existencia de una lucha de clases evolucionada que ha superado los viejos antagonismos de clase de la era industrial: burguesía *vs* proletariado.

Mediante la civilización de los miembros del proletariado como consumidores masivos de una producción masiva, la burguesía se aseguró en el pasado su autoprotección. Ahora, la adopción de tecnología digital en la producción y cultura de masas ha precipitado la nueva estructura de antagonismo de clases y ha generado una paradoja para el poder burgués: "[…] los mismos instrumentos de su comunicación y su cultura establecen las modalidades de la resistencia que se vuelven contra ella misma" (Moglen, 2003a). De modo que las clases trabajadoras del conocimiento —los trabajadores digitales— se radicalizan "por el conflicto entre lo que saben que es posible y lo que la ideología burguesa les compele a aceptar", emergiendo de esa discordancia la consciencia de una nueva clase que debe llevar a la caída de la estructura de producción basada en la propiedad y de la estructura de distribución basada en la coacción del pago. El aislamiento de los creadores, fomentado por el sistema de competencia entre actores, empezaría a ser reemplazado por una

combinación revolucionaria de los mismos, derivada de su asociación y de su colaboración.

Moglen (2003a) argumenta que esta nueva clase, fruto de la asociación libre de creadores y de su modelo anarquista de producción sin propiedad, hace posible la creación de software libre y, por ende, propicia que los creadores tomen el control de la tecnología para producciones subsecuentes y que la Red, liberada de controles, se convierta en el centro neurálgico de un nuevo sistema de distribución basado en la asociación entre pares sin control jerárquico. La liberación de la información del control de la propiedad privada libera al trabajador de su rol impuesto como guardián de la máquina. Proteger la propiedad de ideas requiere suprimir la tecnología libre, lo que conlleva la supresión de la libertad de expresión y la aplicación de un sistema de censura. Frente al ideal de la libre información, la burguesía ha impuesto una sola *libertad*, la del libre comercio —eufemismo neoliberal—, con la que intenta provocar la misma crisis de sobreproducción que alguna vez temió y atrapar a los creadores en su rol de consumidores asalariados y dúctiles. De esta manera, trabajadores y creadores forman una masa incoherente dispersa por todo el mundo y continúan divididos por su competencia. Sin embargo, Moglen se muestra convencido que el uso de la Red facilitará la unión entre ambas clases y la configuración de una economía genuinamente libre.

Para Barbrook, "la libertad de expresión es el libre comercio" genuino (2002: 156), una amenaza a los privilegios privativos y del monopolio del conocimiento burgués. Puesto que no hay una solución tecnológica para la protección de los derechos de autor, los propietarios capitalistas sólo pueden preservar su riqueza de una manera: con el poder del Estado ejercido mediante leyes restrictivas y coercitivas que criminalicen la libre adquisición y distribución de conocimiento (Barbrook, 2002; Moglen 2003a). Este conflicto entre las nuevas clases digitales y la burguesía capitalista encuentra sus orígenes en la "desconfianza en la autoridad" de los hackers y su "tendencia a posicionarse fuera de las normas y valores de la sociedad burguesa" (Hannemyr, 1999). La desconfianza ha evolucionado en confrontación económica, política y social en pro de la libertad de información y, por ende, del individuo.

II.4.1.5. Resistencia a las guerras futuras

Wray (1998) explora la resistencia popular a futuros enfrentamientos bélicos como la tercera transgresión que nos acerca aún más a un escenario de conflicto y nos aleja del ideal de la esfera pública en red. Wray sitúa los orígenes de esta categoría de activismo en el transcurso de la primera guerra del Golfo Pérsico (1990-1991), considerada la primera contienda dominada por las tecnologías digitales de la información y la comunicación, y patrón para las guerras futuras, en las que el objetivo principal son las infraestructuras eléctricas y las redes de comunicación del enemigo (Adams, 1998).

La del Golfo fue la primera guerra controlada por hardware y software. Las armas fueron dotadas con *inteligencia*, los militares empezaron a librarse del dramático combate masivo cuerpo a cuerpo[87] y el Gobierno, de rendir cuentas ante miles de tumbas de soldados caídos en el frente. Y las audiencias fueron extasiadas con imágenes televisidas en tiempo real de un espectáculo bélico diseñado para las pantallas de entretenimiento. Desde entonces, el uso de redes redes informáticas han transformando radicalmente la guerra militar de dos maneras: tecnológicamente y estratégicamente. Al uso de armamento inteligente y de comunicaciones electrónicas se suma un nuevo enfoque estratégico conocido como *swarming*, o ataque de enjambre, una versión de alta tecnología de la vieja guerra de guerrillas que elimina la noción clásica del frente y que permite a pequeñas unidades autónomas, provistas de gran poder de fuero, un buen entrenamiento e información en tiempo real, agruparse en clústers o racimos, con capacidad para concentrar su ataque en un objetivo enemigo durante un espacio de tiempo limitado, infligiendo un gran daño y volviéndose a dispersar posteriormente. Esta modalidad de guerra no lineal, basada en redes, depende totalmente de un sistema de comunicaciones sólido y seguro que permita mantener conectados permanentemente a todos los nodos de la red (Castells, 2001: 184).

La metáfora del enjambre es también válida en Wray (1998) para idealizar el hacktivismo del siglo XXI. Su aplicación es ensayada por primera vez por el Electronic Disturbance Theater[88]. En 1998, Wray vaticina una resistencia civil a las

[87] Los soldados de la coalición heridos en la guerra del Golfo fueron, oficialmente, 776; los fallecidos, 190 por ataque enemigo y 379 por fuego amigo o accidentes. Los muertos iraquíes se contaron por decenas de miles.
[88] Véase página 231.

guerras más generalizada en forma de hacktivismo, que se configura en lo que denomina el quinto portal de entrada a la política de acción directa extraparlamentaria en la Red.

La primera guerra del Golfo es para Wray no sólo un indicativo de un cambio paradigmático hacia la práctica de la guerra de información, sino también de una nueva forma de resistencia a los esfuerzos bélicos de los Estados que es canalizada por las tecnologías de la información y la comunicación. Opositores en Occidente a la guerra del Golfo —principalmente en Estados Unidos— utilizaron el correo electrónico para comunicarse a través de sistemas de tablones de anuncios y grupos de noticias electrónicos, y conocieron la existencia de otros grupos resistentes distanciados geográficamente. Otros que no tenían acceso a computadoras se comunicacaron mediante fax y teléfono. Y los que no tenían acceso a estos grupos de resistencia tecnificada —la mayoría— participaron en las protestas callejeras motivados por la recepción de información canalizada por medios tradicionales, desde el más primitivo boca a boca y la moderna cartelería, hasta medios de comunicación de masas como la radio y la televisión. En realidad, la Red jugó un papel marginal en la diseminación de información y la movilización ciudadana, pues aún estaba en su fase previa a la Web, pero ya estaba anticipando nuevas formas de resistencia civil.

En pleno auge del hacktivismo, en 1998, Wray especula con una futura resistencia hacktivista generalizada en forma de enjambre que permitirá acciones continuas globales, en lugar de las actividades singulares, inconexas y esporádicas que observa en los orígenes del hacktivismo. Esa nueva modalidad de movimientos de resistencia ciberespacial que trascienden las fronteras geopolíticas tradicionales, una resistencia global e incesante, simultánea, ubicua y horizontal, articulada como un enjambre de sujetos contestarios interconectados, es lo que posibilitará, para Wray, la resistencia a la guerra futura, la manifestación de la fuerza real del hacktivismo.

En 1998, Wray reconoce que “no existe un consenso entre los activistas sobre la desobediencia civil electrónica, las acciones hacker con fines políticos, el hacktivismo, o, en general, la política extraparlamentaria de acción directa en la Red”. Las críticas de algunos sectores se centran en el grado de efectividad política, estratégica y técnica de estas tácticas y en si son apropiadas o no desde una visión ética, política y legal. Wray pregunta: “¿Qué será del hacktivismo cuando pase de estar

integrado por incidentes aislados a convertirse en una convergencia de fuerzas aliadas? ¿Desaparecerá entonces el hacktivismo y se transformará en resistencia ciberespacial?". La respuesta la obtuvo sólo un año después con la irrupción del movimiento antiglobalización, que extendió a la economía los conceptos de guerra injusta y de resistencia a ésta. Lo cierto es que Wray ya había anticipado que el hacktivismo evolucionaría "de acuerdo con los cambios que se operen en las condiciones mundiales económicas y políticas" (Wray, 1998).

II.4.2. Primeros estudios académicos

En los albores del siglo XXI se publican los primeros estudios académicos relevantes sobre hacktivismo. Uno de ellos es el de Samuel (2004), quien ofrece una matriz taxonómica sobre el hacktivismo con apoyo empírico. Las tres categorías que propone se basan en los orígenes y orientaciones de los actores participantes en cada una de ellas.

Cuadro 5: Matriz taxonómica del hacktivismo propuesta por Samuel (2004).

	Formas	**Orígenes**	**Orientación**
***Cracking* Político**	Desfiguraciones Redirecciones Ataques DDoS Robo de información	Programadores hackers	Delictiva
Hacktivismo Performativo	Parodias Sentadas	Artistas activistas	Transgresora
Código Político	Desarrollo de software	Programadores hackers	Transgresora

Fuente: elaboración propia a partir del trabajo de Samuel (2004).

Para Samuel (2004: 36), los orígenes del *cracking* político y de la codificación política se encuentran en la cultura computacional hacker, mientras que las raíces del hacktivismo performativo se hallan en la cultura postmoderna de izquierdas, en concreto, en las actividades de artistas activistas progresistas.

Las sentadas virtuales en apoyo a los zapatistas son ejemplos de hacktivismo performativo, en la taxonomía de Samuel. La codificación política —desarrollo de software con fines políticos— encuentra sus manifestaciones más tempranas en las acciones de Cult of the Dead Cow y su creación de programas informáticos como Peek-a-Booty para evadir la censura, o en las más actuales de WikiLeaks y su uso de sistemas encriptados para proteger las identidades de su red de confidentes y las comunicaciones de sus colaboradores. Los ataques DDoS[89] organizados por los *electrohippies* contra la Organización Mundial del Comercio durante las protestas de Seattle, en 1999, o las acciones de Anonymous, en su vertiente computacional, son ejemplos de *cracking* político, en la terminología y taxonomía propuestas en la tesis de Samuel. Pero también observamos que la heterogeneidad y transversalidad de Anonymous origina la existencia de subgrupos dedicados al hacktivismo performativo, en el que podemos incluir también acciones artísticas. Ejemplo de esto es Anonymous ART of Revolution, inspirada en la idea de Anonymous y el movimiento *Occupy*, cuya página en Facebook supera el millón de fans. Su leyenda: "El arte no existe sólo para entretener, sino también para desafiar a uno a pensar, para provocar, incluso para perturbar, en una constante búsqueda de la verdad".

Ilustración 8: Portada de Anonymous ART of Revolution en Facebook.

Fuentes: https://www.facebook.com/Anonymous-ART-of-Revolution-362231420471759/.

Las investigaciones de Jordan y Taylor sobre el hacktivismo han sido las más minuciosas y sustanciales desde la perspectiva de la desobediencia civil electrónica y

[89] DDoS son las siglas en inglés de Distributed Denial of Service (ataque distribuido de denegación de servicio). Esta acción consiste en atacar un servidor de manera conjunta y coordinada desde varios equipos para que deje de funcionar.

el activismo en el ciberespacio. En su trabajo conjunto descomponen el hacktivismo en dos corrientes de acciones: el hacktivismo de acción de masas —o acción directa de una masa virtual— y el hacktivismo digitalmente correcto. Estas dos categorías no deben tomarse como entidades totalmente separadas, sino como corrientes o tendencias del movimiento hacktivista en su conjunto que interactúan y entran en conflicto entre sí (Jordan y Taylor: 2004: 116).

Para estos dos autores, el hacktivismo de acción de masas es sinónimo de la desobediencia civil electrónica introducida por Wray (1998, 1999) y experimentada en sus formas más primitivas por el Electronic Disturbance Theater y toda una suerte de activistas forjados en formas clásicas de protesta y desobediencia civil. Estos nuevos ciberactivistas descubrieron en la ética hacker un paraguas y en las tecnologías digitales y el ciberespacio, la posibilidad de aplicar nuevas estrategias y tácticas de resistencia y contestación más efectivas, mediante la ejecución de acciones directas ubicuas, inmediatas, persistentes y masivas. Jordan y Taylor reconocen los orígenes de esta forma de hacktivismo en la participación de hackers y activistas digitalizados en el movimiento antiglobalización, a partir de la segunda mitad de la década de 1990, contribuyendo a generar un clima de beligerancia civil permanente en todo el mundo contra gobiernos y organismos supranacionales valedores del capitalismo neoliberal (Fondo Monetario Internacional, Banco Mundial, G8, Organización Mundial del Comercio, etc.).

Hackers y activistas digitalizados jugaron un papel decisivo en las manifestaciones antiglobalización masivas que se produjeron en todo el mundo a finales del siglo XX y en la primera década del XXI (Chiapas, Seattle, Génova, Barcelona, Washington, Praga, Gotemburgo, Salzburgo, Rostock, Bangkok…). También articularon en el ciberespacio redes hacktivistas reactivas y proactivas y fueron fundamentales en la irrupción de nuevos medios de comunicación alternativos en Internet —organizados en la red global de contrainformación Indymedia— y en la configuración de espacios abiertos, descentralizados y en red para la participación y el debate civil global, cuyo máximo exponente ha sido desde el año 2001 el Foro Social Mundial, un enorme laboratorio de ideas contra el neoliberalismo y la dominación del mundo por el capital y cualquier forma de imperialismo. Las acciones prozapatistas y las protestas contra las cumbre de la Organización Mundial del Comercio en 1999 —

conocidas como la batalla de Seattle— han sido encumbradas como los paradigmas del hacktivismo de masas.

Los hacktivistas de acciones de masas rechazan la mercantilización de las tecnologías ciberespaciales y se resisten a usarlas de acuerdo a las normas de eficiencia establecidas por las sociedades capitalistas virales (Jordan y Taylor, 2004: 163). Perp para estos dos autores, esta forma de activismo hacker incurre en una paradoja: busca ser legitimado con el apoyo de las masas, pero al recrear esos cuerpos físicos en el ciberespacio está rechazando algunos de los poderes inmanentes de este espacio virtual; es decir, implementa formas limitadas del poder ciberespacial para garantizar que sus acciones sean vistas como una política de masas (Jordan y Taylor, 2004: 4).

Por su parte, el hacktivismo digitalmente correcto ha radicalizado las obsesiones originales de la comunidad hacker relativas al acceso universal a la información, a que ésta fluya libremente y a que tanto emisores como receptores dispongan de las capacidades y herramientas necesarias para proteger la privacidad de sus comunicaciones.

Los hacktivistas han importado para la comunidad hacker las preocupaciones sobre la globalización neoliberal y sus efectos en los Estados-nación y sus sociedades, pero con un enfoque informacional, en particular, en lo relativo a la aplicación de mecanismos de censura y control en Internet. Es por ello que Jordan y Taylor observan en sus acciones manifestaciones de una política informacional que fluye en la virtualidad y que está vinculada a los poderes inherentes del ciberespacio (Jordan y Taylor, 2004: 4, 90-115).

Aunque sus métodos sean diferentes y a veces puedan incluso entrar en conflicto —en función de la lectura interpretativa que se haga de la ética hacker—, lo cierto es que ambas corrientes —la acción directa de una masa virtual y la acción digitalmente correcta de una elite hacker informática— "forman parte del hacktivismo y el hacktivismo es pura política informacional para los tiempos informacionales" (Jordan y Taylor, 2004: 163).

> Los hacktivistas digitalmente correctos están interesados en la información no sólo por su deseo de mantener capacidades contra la censura en el ciberespacio, lo hacen porque hay personas encarceladas, reprimidas y dañadas por el uso de la censura en sus Estados-nación. Los hacktivistas de la acción de masas están

> preocupados por propagar reuniones masivas de cuerpos virtuales no sólo por su deseo de ver la desobediencia civil y la resistencia operando en vidas virtuales, lo hacen en apoyo de personas que están siendo encarceladas, reprimidas y dañadas en sus vidas virtuales y no virtuales. El hacktivismo aborda la política, virtual y no virtual (Jordan y Taylor, 2004: 171-172).

Jordan y Taylor concluyen que los hacktivistas, en su conjunto, abordan en última instancia las miserias y la falta de derechos humanos, y representan la resistencia en los tiempos virales, el primer movimiento social virtual (2004: 171-172).

Atendiendo a la matriz taxonómica aportada por Samuel y a la categorización de Jordan y Taylor, consideramos oportuno actualizar sus propuestas con una nueva categoría: el hacktivismo informacional. El estudio de Samuel es previo a la aparición de WikiLeaks y de una nueva forma de hacktivismo que incluye nuevas tácticas relacionadas con el manejo estratégico de información, su difusión y sus efectos en la opinión pública. Los análisis de Jordan y Taylor, por su parte, aunque también anteriores a WikiLeaks, ya avanzan un tipo de hacktivismo con un enfoque informacional, pero limitado en sus estudios al uso de código político. Veremos en el capítulo IV, dedicado a nuestro caso de estudio, WikiLeaks, cómo el nuevo hacktivismo informacional amplía las estrategias y herramientas para amplificar su impacto.

II.5. GÉNESIS HACKTIVISTA

II.5.1. De los *yippies* a la Electronic Frontier Foundation

Durante la década de 1980 y la primera mitad de 1990, grupos de hackers como el Chaos Computer Club, Cult of the Dead Cow o la revista *2600*, y organizaciones como la Electronic Frontier Foundation generaron el caldo de cultivo para la emergencia del hacktivismo. Pero antes que ellos, una generación anterior de hackers ya empezó a *jugar* con el potencial político del *hacking*.

Los valores inherentes al *hacking* —ilustrados en la ética hacker— han estimulado, desde sus orígenes, el desarrollo de la conciencia política de esta comunidad y su manifestación pública. Si bien es cierto que la dimensión lúdica del *hacking* prevaleció sobre la política en la primera generación de hackers, en éstos ya se intuían motivaciones políticas radicales en su deseo de democratizar la tecnología y las telecomunicaciones, en su afán por facilitar el acceso ilimitado al poder de la computación y la difusión libre de información (Jordan y Taylor, 2004: 13). Frente aquéllos más fascinados por la dimensión lúdica del *hack* y por cuestiones puramente tecnológicas que en apariencia los distanciaban de preocupaciones sociales, una corriente de *phreaks* y hackers informáticos cada vez más comprometidos con los usos sociales de la tecnología y su orientación política empezó a emerger a finales de la década de 1960 y principios de los años setenta.

Parece haber cierto acuerdo en identificar en el movimiento contracultural *yippie* estadounidense las raíces del *underground* hacker y las manifestaciones más primitivas de hacktivismo (Sterling, 1992; Jordan y Taylor, 2004; Goldstein, 2009). Los *yippies* fueron una suerte de escindidos excéntricos y radicalizados del movimiento *hippy*, libertarios, antiautoritarios, anarquistas de izquierdas, apologistas de la promiscuidad y del consumo de drogas, y también *phreaks*. Su líder, el escritor y activista Abbie Hoffman, fundó en 1967 el Youth International Party, un partido que predicaba el anarcocomunismo, el antiautoritarismo y el antimilitarismo mediante una política simbólica que mezclaba teatralidad, comicidad y surrealismo. Frente al ruralismo contemplativo y el primitivismo de los *hippies*, los *yippies* optaron por la acción directa en las urbes y el uso de herramientas tecnológicas modernas para sus campañas de agitación. Por ejemplo, utilizaron chapas de metal como monedas falsas para usar los teléfonos públicos de pago como táctica de desobediencia civil al

impuesto extra que el Gobierno de Estados Unidos había aplicado al servicio telefónico para financiar la guerra en Vietnam.

En mayo de 1971, Hoffman y un entusiasta de los teléfonos autodenominado sarcásticamente Al Bell pusieron en marcha el boletín de noticias *Youth International Party Line*, conocido popularmente como *YIPL*. Esta pionera revista *phreak* es reconocida como el primer medio de información hacker de la historia (Hoffman, Bell y Edison, 2010). El boletín, gratuito, difundió entre 1971 y 1984 consejos prácticos que iban desde artimañas para realizar llamadas gratis desde teléfonos públicos, hasta técnicas de *lock-picking*. El objetivo fundamental era acabar con el monopolio corporativo de la Bell Telephone Company. Fruto de su progresivo distanciamiento del *yippismo*, y con la intención de iniciar una nueva etapa más centrada en aspectos técnicos que en políticos, Al Bell rebautizó el boletín en septiembre de 1973 con el nombre *TAP*, traducido primero como *Technological American Party* y, posteriormente, como *Technological Assistance Program* cuando Tom Edison se hizo cargo de su edición en 1979.

El final de *TAP*, en 1984, coincidió con la aparición se mismo año de la revista *phone-phreak/hacker 2600*. Su editor, Eric Gordon Corley —un "disidente" que tomó para sí el nombre de Emmanuel Goldstein, el enigmático personaje de la novela *1984* de George Orwell, como "síntoma de la gravedad de su visión sociopolítica del mundo" (Sterling, 1992)— recogió el testigo de *TAP* para poner en marcha este proyecto editorial que se ha convertido en el gran archivo hacker estadounidense de las últimas tres décadas.

> *TAP* fue la primera publicación en ofrecer una mirada hacker a la tecnología. *2600* difícilmente existiría en su forma actual sin la inspiración ofrecida por *TAP* (Goldstein, 2009: 229).

Es en la década de 1980 cuando se consolida una escisión en la cultura hacker, con dos grupos claramente diferenciados: por un lado, el que se introduce en el *mainstream* y mercantiliza sus habilidades y conocimientos, desarrollando software y hardware privativos, y por otro, el que configura el *underground* computacional, que se mantiene fiel a la ética hacker, crea software y hardware libres, y desarrolla una dimensión política que prepara el terreno para la emergencia del hacktivismo. La revista *2600* ha sido desde 1984 uno de los principales altavoces del segundo grupo,

de los *auténticos* hackers. El compromiso político cada vez más activo de esta comunidad, las crecientes redadas y arrestos de hackers, y las demandas interpuestas por el imperio corporativo contra Goldstein y su publicación abrieron cada vez más espacios al discurso político en esta revista, a las llamadas al activismo y a la defensa de la libre información y de la ética hacker.

> Hablamos de la libertad: la libertad para explorar, para ser un individuo, para difundir información a través de cualquier medio disponible. Y todo eso continua hoy y continuará en el futuro indefinido. Es parte de lo que somos, no como hackers, sino como seres humanos (Goldstein, 2009: 207).

La línea editorial de *2600* se ha ido caracterizando cada vez más por un "tono antiautoritario" que mantiene que "dispositivos, leyes o sistemas que prohíban el acceso al conocimiento y su libre distribución son provocaciones que cualquier hacker libre y digno debe atacar implacablemente" (Sterling, 1992).

Tanto *YIPL/TAP* como *2600* han sido una exaltación literaria de la dimensión política que subyace en el *phreaking*, en particular, y en el *hacking*, en general. Una de las aportaciones más notables en este sentido es la de Sterling cuando identifica tintes políticos en la subversión y manipulación del sistema telefónico, equiparables a los que se hallan en el *hacking* computacional. En el contexto estadounidense —pero aplicable a cualquier Estado bajo el imperio del capitalismo tecnológico—, este autor reconoce en las computadoras y en los teléfonos unos "poderosos símbolos de la autoridad organizada y de la elite de negocios tecnocrática" (Sterling, 1992). De ahí que cualquier intento por subvertir un sistema de seguridad telefónico o informático es también una tentativa de penetrar en la zona de confort del poder autoritario para subvertirlo, aflorando así la dimensión política del *hacking* telefónico e informático, que cada vez se hizo más explícita en el transcurso de la década de 1980.

La aparición en 1984 de la revista *2600* coincidió con la fundación ese mismo año en Lubbock (Texas) de Cult of the Dead Cow, el primer grupo hacktivista de la historia, que acuñó el término *hacktivismo* en el año 1994. Cult of the Dead Cow se ha hecho famoso por el desarrollo de herramientas gratuitas hacker y hacktivistas, su voluntad de discutir sus puntos de vista públicamente y su compromiso con los principios del llamado hacktivismo digitalmente correcto (Jordan y Taylor, 2004: 97-98).

Cult of the Dead Cow se autodefine como un laboratorio de ideas sobre la privacidad y la seguridad en la Red, y se jacta de haber sido "una fuerza innovadora en el *underground* informático" y de haber lanzado la "primera publicación electrónica" de la historia, en 1984. En el tono bromista y satírico que caracteriza la mayor parte de los textos de su página web —síntoma del espíritu *juguetón* del hacker—, este grupo multidisciplinar explica:

> La Gran Dinastía Imperial cDc incluye a un exasesor presidencial sobre seguridad informática, un investigador de Harvard, un exfuncionario de la ONU, un asistente de fiscal de distrito, un profesor de lógica, un cineasta galardonado, varios autores publicados, un desarrollador de videojuegos, un Eagle Scout [el rango más alto en Boy Scouting], programadores de todo tipo, artistas gráficos, músicos, operadores de divisas y un merovingio (Cult of the Dead Cow, 2004).

Varios integrantes de Cult of the Dead Cow han sido también miembros de otros grupos y laboratorios hackers, y de asociaciones de profesionales de las telecomunicaciones, ingeniería informática e investigación científica. La lista es diversa: L0pht, Institute for Electrical and Electronics Engineers, Legion of Doom, Association of Computing Machinery, Hasty Pastry, Restricted Data Transmissions, Masters of Deception, USENIX Association, Walnut Factory, Soylent Communications, Institute for Operations Research and the Management Sciences, New Hack City y Youth International Party Line/Technology Assistance Program.

Las aportaciones de Cult of the Dead Cow han sido decisivas para la cultura hacker y el *underground* informático, especialmente para el desarrollo del hacktivismo y de una nueva estructura social y económica basada en la cooperación, la libre información, la libertad de expresión, la privacidad y la seguridad en las comunicaciones. En 1990, Cult of the Dead Cow creó la HoHoCon, considerada la primera convención hacker moderna en Estados Unidos, que se celebró hasta 1995 en Houston (Texas). En 1994 se convirtió en el primer colectivo *undergound* de computación en tener su propio grupo de noticias de Usenet. En 1996 fundó Ninja Strike Force, un subgrupo *ninja* formado por "la elite de la elite", dedicado a la consecución de los objetivos de este grupo hacker.

En 1997, Cult of the Dead Cow ya distribuía música original en formato MP3 en su sitio web, adelantándose al fenómeno Napster y al furor de los sistemas de intercambio, descarga y *streaming* de archivos musicales en la Red. Su primer archivo

MP3 compartido fue el tema *Kingpin*, de Weasel-MX, la banda de Grandmaster Ratte', uno de los fundadores de Cult of the Dead Cow. El tema se grabó con dos ordenadores Commodore Amiga, un teclado Casio, la guitarra de Lee Shiftlet y un grabador de casetes de cuatro pistas.

En 1998, estos hackers lanzaron Back Orifice, un programa de control remoto creado para dejar en evidencia a Microsoft (y al capitalismo tecnológico) y abrir los ojos de los consumidores sobre la seguridad de sus sistemas operativos. Back Orifice fue diseñado como un sistema de administración remota de computadoras y redes que permite a un usuario controlar un ordenador a través de una red local o de Internet, mediante el protocolo de comunicaciones TCP/IP. Su primera versión funcionaba únicamente bajo Windows 95 y Windows 98; más tarde se lanzó la versión BO2K para Windows NT y Windows 2000.

Cult of the Dead Cow dio el paso más decisivo hacia el activismo hacker en el año 1999, al auspiciar la creación del grupo internacional Hacktivismo para la creación de tecnología anticensura y la promoción de los derechos humanos en Internet. En el año 2002, presentaron en la CodeCon en San Francisco el software político Peek-a-Booty, que permite la transmisión libre en Internet de información cifrada *peer-to-peer* eludiendo cualquier forma de control o censura en la Red. El software se creó especialmente para aquellos individuos y organizaciones que operan en países donde se socavan los derechos de libre expresión e información, permitiéndoles cifrar sus contenidos y proteger las identidades tanto de los emisores como de los receptores.

Mientras, en Europa, la fundación el 12 de septiembre de 1981 del Chaos Computer Club —en la parte oeste del Berlín dividido por el muro de la vergüenza— fue uno de los pasos más decisivos hacia el activismo político hacker. En los primeros años de la década de 1980, Europa asistió a la emergencia de una nueva generación de hackers que se constituyó en comunidad y que abordó directamente las implicaciones políticas de una de las consignas hackers más repetidas: "Toda la información quiere ser libre". Desde un principio, el Chaos Computer Club reivindicó la libre comunicación, el flujo libre de información y el acceso universal al conocimiento como derechos humanos básicos y necesarios para el desarrollo de una auténtica sociedad de la información (Jordan y Taylor, 2004: 14). La conciencia política de los

hackers europeos —en particular, la de los pioneros alemanes— era más acusada que la de sus semejantes estadounidenses. En otoño de 1989, Goldstein ya observó que el *hacking* era "mucho más político en Alemania Occidental que en cualquier otro país" (Goldstein, 2009: 217).

El Chaos Computer Club surgió para proveer servicios e información sobre cuestiones técnicas y sociales relacionadas con la vigilancia, la privacidad y el anonimato, las infraestrucuras de comunicación, la libertad de información, el activismo hacker, la seguridad de datos y demás temas relacionados con la tecnología y la ética hacker. Estos temas han sido tratados también en su revista *Datenschleuder*, creada en 1984 por Wau Holland, cofundador del Chaos Computer Club.

El *paritorio* donde nació el club hacker más influyente y longevo de Europa fue la sede del periódico alemán *Die Tageszeitung*, una publicación alternativa, izquierdista y ecologista fundada en 1978 y cuyo modelo de gestión es cooperativo. Esto evidencia la naturaleza política progresista y cooperativa dominante en la segunda generación hacker y muestra también que los hackers políticamente más comprometidos han sentido la imperiosa necesidad de mantener una relación umbilical con el periodismo y de usar los medios de comunicación de distintas formas en diferentes épocas para expresarse, hacerse comprender, difundir sus conocimientos, denunciar negligencias en materia de seguridad informática y abusos de poder, y contribuir al debate público sobre el uso de las tecnologías digitales y su influencia social.

Desde los primeros boletines informativos autogestionados de la década de 1970, hasta la asociación interesada de WikiLeaks con grandes corporaciones mediáticas, o el uso de YouTube y las redes sociales en línea por Anonymous, pasando por la autoedición de revistas como *2600* y *Datenschleuder* —ambas, herederas de *TAP*—, o la aparición de los primeros medios alternativos en línea como el de Cult of the Dead Cow, hemos asistido a toda una variedad de estrategias y formas comunicativas e informativas de los hackers activistas sobre las que apenas se ha arrojado luz científica. Este interés en el uso de los medios de comunicación para conectarse con la sociedad se hizo evidente en noviembre de 1984, cuando los hackers Wau Holland y Steffen Wernéry descubrieron una vulnerabilidad en el recién estrenado servicio en línea Bildschirmtext (Btx), un sistema de teletexto interactivo

propiedad del Bundespost, el servicio postal germano, que transmitía datos a través de la red telefónica. Los hackers del Chaos Computer Club avisaron a los gestores de esta red de la falla en el sistema implementado por IBM, en el que se había invertido más de 700 millones de marcos (moneda alemana antes de la entrada del euro). Pero los dos hackers fueron ignorados, así que decidieron ridiculizar al Bundespost ante la opinión pública: Holland y Wernéry entraron en la red, consiguieron los datos de la caja de ahorros Hamburger Sparkasse AG y cargaron a ésta 134.000 marcos[90] en donaciones al Chaos Computer Club. Luego, los hackers se pusieron en contacto con la ZDF —televisión pública alemana— para dar a conocer este hecho, dejar en evidencia el sistema del servicio postal y devolver el dinero. En su defensa, los hackers explicaron que sólo querían demostrar que el sistema Btx era vulnerable y podría ser atacado por auténticos delincuentes cibernéticos. Aquel incidente dio a conocer al Chaos Computer Club.

> Bajo la presidencia de Holland —y posteriormente sin él— el CCC se caracterizó por este uso de los medios de comunicación para denunciar casos de inseguridad informática donde, sin la presencia de los mismos, la denuncia podría haber puesto en peligro al grupo. Así, entre otros el CCC ha demostrado públicamente fallos en diversos sistemas informáticos, como la tecnología ActiveX de Microsoft en 1996 o la clonación de tarjetas GSM en 1998. En marzo de 2008 consiguieron y publicaron la huella dactilar del entonces ministro del Interior germano, Wolfgang Schäuble, en protesta por el uso de datos biométricos en los e-pasaportes de Alemania (Molist, 2014).

Todas estas transgresiones encontraron un complemento vitamínico en la aparición en 1990, en Estados Unidos, de la Electronic Frontier Foundation, organización que canalizó las preocupaciones políticas de la comunidad hacker en la clandestinidad hacia un nuevo espacio abierto de confrontación directa con el poder del Estado-nación. Su aparición supuso el nacimiento del libertarismo civil electrónico (Sterling, 1992) y fue fundamental para la formulación de lo que Himanen (2001) llama la nética —o ética de la Red—, el tercer plano significativo de la ética hacker, junto con la ética del trabajo y del dinero.

La Electronic Frontier Foundation fue la primera institución política de la Red, la primera organización para la defensa de los derechos civiles en el ciberespacio, la primera misión para sacar de la clandestinidad al *underground* computacional y

[90] El marco fue primero la moneda oficial de la Alemania Occidental y, luego, de la Alemania unificada tras la caída del Muro de Berlín, hasta la entrada del euro, el 1 de enero de 2002.

legitimarlo ante la opinión pública, interviniendo en la esfera pública como nuevo grupo de presión.

Las raíces de la Electronic Frontier Foundation se hunden en el libertarismo y la ética hacker. Sus fundadores fueron cinco filántropos de la segunda ola de hackers (Hannemyr, 1999): John Perry Barlow, Mitch Kapor, Steve Wozniak, John Gilmore y Stewart Brand. Los vínculos y compromisos de la Elecronic Frontier Foundation con la cultura hacker son tan profundos, que su propio nacimiento fue una respuesta a la *Operación Sun Devil* en Estados Unidos, el primer embate policial a gran escala contra hackers, que tuvo lugar entre el 7 y 8 de mayo de 1990. Pero los objetivos de la Electronic Frontier Foundation han sido más amplios que la mera defensa de los hackers perseguidos por la autoridad. La defensa de la libertad de expresión y de la privacidad en Internet, y la lucha contra el control gubernamental de la Red son los principios libertarios sobre los que esta organización ha sostenido su existencia (Castells, 2001: 66).

Barlow —letrista del grupo musical Grateful Dead e hijo de la contracultura estadounidense de la década de 1960, afín al Partido Republicano y reconvertido en periodista informático en la década de 1980— se convirtió en un pionero del movimiento por los derechos en el ciberespacio y en el primer comentarista púlico en aplicar el término *ciberespacio* —creado por William Gibson en su novela *Neuromancer*— para expresar el espacio virtual y fronterizo que surge del nexo entre dispositivos computacionales y redes de comunicación electrónicas, que exige un nuevo conjunto de metáforas, un nuevo conjunto de reglas y comportamientos (Sterling, 1992; Himanen, 2001: 86).

Kapor es una de las figuras más importantes en el desarrollo de las computadoras personales. En 1982, creó el programa de hoja de cálculo Lotus 1-2-3, presentado para ordenadores IBM en 1983. Este software fue "la primera aplicación informática que simplificó notablemente una función de uso común, lo cual constituyó un factor importante en la implantación del ordenador personal" (Himanen: 2001: 86). Esta aplicación fue el primer producto de Lotus Software, empresa fundada por Mitch Kapor y Jonathan Sachs y emblema del sector del software en la década de 1980. Kapor, desmotivado, dejó el negocio al cabo de cuatro años.

Tanto Kapor como Barlow fueron investigados por el FBI en relación a la

distribución del código de un software privativo de Apple. En junio de 1989, alguien autodenominado NuPrometheus, que decía actuar en nombre de una misteriosa y nunca conocida organización *fantasma* denominada Nu Prometheus League, envió un disquete a personas relacionadas con la industria de la computación que contenía un fragmento del código fuente del software Color Quickdraw, propiedad de Apple Computer, empresa cuyos padres fundadores —Steve Jobs y Steve Wozniak— ya habían abandonado. Aunque aquel fragmento de código era inútil, inoperable en términos de reutilización, su liberación fue "una bofetada, deliberada y simbólica en la cara de la jerarquía corporativa de Apple" (Sterling, 1992).

En mayo de 1990, Barlow recibió la visita de un agente local del FBI de Wyoming para interrogarle sobre el caso de NuPrometheus. Según Barlow (1990) y Sterling (1992), el FBI buscaba a los asistentes de "un grupo sospechoso" y "clandestino" de hackers que se reunían en The Hackers' Conference en San Francisco y que tendrían, según los agentes federales, vínculos con la Nu Prometheus League. Barlow no fue arrestado ni acusado de ningún crimen, pero aquel encuentro con el FBI le llevó a explicar su experiencia en The WELL (The Whole Earth 'Lectronic Link), un BBS emanado en 1985 de la Point Foundation, fundación creada en 1972 por el millonario libertario Steward Brand —también creador de The Hackers' Conference— para canalizar el esfuerzo de los libertarios civiles.

En 1990, The WELL tenía cerca de cinco mil usuarios y ya había sido escenario de intensos debates centrados en el *hacking*, participados por hackers y libertarios del *underground* informático como el propio Barlow, Acid Phreak o Phiber Optik. A modo de ensayo breve, Barlow relató en el BBS su encuentro con el FBI y no tardó en tener una gran repercusión en la comunidad de The WELL. Uno de sus usuarios más impresionados por aquel relato fue Mitch Kapor, que estaba viendo con enorme preocupación cómo por todo el país se iba desarrollando una operación antihackers. En junio de 1990, aún impactados por el desarrollo de la *Operación Sun Devil* —la mayor redada hacker hasta el momento— Barlow y Kapor se reunieron en la oficina del primero, en Pinedale, Wyoming, para tratar estos temas, convencidos de que la guerra contra los hackers suscitaba importantes cuestiones sobre libertades civiles constitucionales. Aquel fue el inicio de la Electronic Frontier Foundation (Sterling, 1992). Inmediatamente, Barlow escribió y publicó el 8 de junio de 1990 el

manifiesto *Crime and Puzzlement* para anunciar que estaban constituyendo legalmente una organización política cuyos objetivos prioritarios serían la educación en los nuevos valores que deberían impregnar el ciberespacio, el cabildeo, la denuncia de cualquier tipo de censura y control en el ciberespacio, y la defensa legal de individuos, colectivos u organizaciones en áreas relacionadas con la libre expresión, el libre acceso al conocimiento, la privacidad y cualquier derecho constitucional extensible a la Red (Barlow, 1990; Sterling, 1992).

El manifiesto libertario corrió como la pólvora a través de canales de redes de computadoras y se imprimió en *Whole Earth Review*, la revista fundada en enero de 1985 tras la fusión de las publicaciones *Whole Earth Software Review* (suplemento del *Whole Earth Software Catalog*) y *CoEvolution Quarterly*, todas ellas descendientes de la revista contracultural *Whole Earth Catalog* creada por Stewart Brand en 1968. El manifiesto de Barlow fue la "réplica coherente y politizada desde las filas hackers" que "electrizó a la comunidad" (Sterling, 1992).

Inmediatamente, Steve Wozniak —cofundador de Apple y creador del primer ordenador personal— y John Gilmore —libertario defensor de sistemas robustos de encriptación, fundador de la lista de correo *Cypherpunks* y de la empresa Cygnus Solutions, y uno de los principales contribuidores del proyecto GNU— ofrecieron su apoyo al proyecto. A estos se sumaron luego Stewart Brand —fundador de la Point Foundation—, los pioneros en realidad virtual Jaron Lanier y Chuck Blanchard y el inversor en redes Nat Goldhaber (Sterling, 1992).

Así fue como nació esta organización, sin ánimo de lucro y no partidista, para la defensa del interés público y para proteger las libertades civiles fundamentales en el ciberespacio, incluidas la privacidad y la libertad de expresión. La primera batalla de la Electronic Frontier Foundation fue la defensa legal de Craig Neidorf, editor de *Phrack*, en el caso del documento del sistema de emergencias E911 publicado en esta revista, recordado en el Capítulo I de esta tesis. La Electronic Frontier Foundation se convirtió así en catalizador de las preocupaciones cada vez más extendidas en la contracultura digital sobre la libertad de expresión, la privacidad y la defensa de los valores de la ética hacker.

II.5.2. Primeras campañas hacktivistas y su irrupción en los medios

En la segunda mitad de la década de 1990, más y más hackers empezaron a participar activamente en acciones electrónicas en red con tintes políticos, en dos direcciones: 1) principalmente, acciones de protesta contra la criminalización y detenciones de hackers, y en defensa de la neutralidad de la Red y la libre información, y 2) acciones en defensa de los intereses de colectivos, comunidades, sociedades y territorios amenazados por abusos de poder estatales y corporativos. La aparición del grupo Internet Liberation Front y la campaña 'Free Kevin' que auspició la revista *2600* son paradigmas del primer caso; el apoyo de los hacktivistas a los zapatistas es paradigma del segundo.

En otoño de 1994, un grupo autodenominado Internet Liberation Front se dio a conocer por la publicación de un manifiesto contra el control corporativo y estatal de Internet y por sus amenazas y ataques al periodista Josshua Quittner, coautor del libro *Masters of Deception: The Gang that Ruled Cyberspace* (1995). Los integrantes de Internet Liberation Front se autodefinían como "una pequeña organización clandestina de expertos en seguridad informática", con las habilidades necesarias para "penetrar prácticamente cualquier red conectada a Internet" y que había "declarado la guerra a cualquier empresa sospechosa de contribuir a la desaparición definitiva de Internet" como espacio indemne al poder y al control de las corporaciones capitalistas más poderosas del mundo. Además, los miembros de este grupo consideraban que los periodistas que escribían sobre hackers, no eran más que "analfabetos computacionales codiciosos", como Quittner, a quien identificaron como "el paradigma del periodismo inexacto y de la estupidez general" (Gilboa, 2001).

Con motivo de la publicación en la revista *Wired* de un adelanto del libro de Quittner y Slatala, Internet Liberation Front llenó el buzón de correo electrónico de Quittner de mensajes y manipuló su línea telefónica y mensajes de voz para que cualquiera que llamase al periodista escuchase una serie de obscenidades. La revista *2600* se hizo eco de la aparición de este grupo en su edición de invierno 1994/1995, en un artículo muy crítico con este grupo por contravenir la ética hacker:

> Ahora parece un momento perfecto para que brote un grupo de activistas para evitar que la Red sea subvertida por la comercialización y el exceso de reglamentación. El manifiesto de un grupo llamado Internet Liberation Front da la impresión de un mordaz, y arrogante idealismo. Eso es exactamente lo que

> necesitábamos. Sin embargo, en lugar de atacar el verdadero enemigo del pensamiento independiente, ¡este grupo anónimo decidió ir tras el autor de un libro! Josh Quittner, cuyo libro sobre hackers, *Masters of Deception*, saldrá a la venta en enero, vio cómo su buzón de Internet se inundaba de manifiestos de ILF. Además, su línea telefónica fue reenviada a un mensaje obsceno. Típicas travesuras de hackers que probablemente nunca habrían sido tomadas en serio, salvo que esta vez fueron hechas por un grupo con un manifiesto. Eso es realmente todo lo que se necesita para escribir titulares en estos días. Esperamos ver uno de estos días la aparición de un grupo que reconozca la importancia de la libertad de expresión y del poder del individuo. Un grupo que no esté financiado por empresas de telefonía, como ciertas organizaciones de «libertades civiles», un grupo que no vea la obra de un autor como una amenaza para la comunidad. Las ideas, incluso cuando son totalmente equivocadas, son una puerta al debate. Las acciones, sin embargo, llevan consigo la amenaza real (Goldstein, 2009: 558-559).

A Internet Liberation Front también se le atribuyeron acciones en noviembre de 1994, en el Día de Acción de Gracias, contra General Electric, NBC, IBM y el proveedor de acceso a Internet Pipeline Network Inc., que tuvo que suspender su servicio durante seis horas, además de otra intervención en el sitio web que Metro-Goldwyn-Mayer había creado para la promoción de la película *Hackers* (1995), dirigida por Iain Softley y protagonizada por Jonny Lee Miller, Angelina Jolie, Renoly Santiago, Matthew Lillard, Lorraine Bracco y Fisher Stevens. Sobre una fotografía promocional de Angelina Jolie y Jonny Lee Miller, los hackers sustituyeron el eslogan original "Este va a ser un sitio promocional entretenido y divertido para una película" por "¡Este va a ser un sitio promocional aburrido y cursi para una película!".

Para Adams (1998: 164), la disrupción y confrontación directa radical de Internet Liberation Front fue el contrapunto a la tradicional vía anglosajona del cabildeo por la que había optado la Electronic Frontier Foundation, aunque ambas compartían un mismo fin: mantener las manos del Gobierno fuera del ciberespacio, tanto como fuese posible, para dejarlo crecer libre.

Más impactante y notoria fue la campaña en la que participaron hackers de todo el mundo en defensa de Kevin Mitnick tras su arresto. A finales de 1997, un grupo hacktivista denominado Pants/Hagis Alliance lanzó un mensaje en el servidor de Yahoo! en el que advertía de la invasión irremediable, el día de Navidad, de un virus en la Red que iba a causar verdaderos estragos y cuya *pócima* sólo sería revelada si Mitnick era liberado. Aunque lograron acceder al servidor, no causaron daños. Fue una demostración de lo que podían hacer los hacktivistas. En 1998 se sucedieron las

amenazas e incursiones hacktivistas en apoyo a Mitnick, afectando al sistema informático de Naciones Unidas o al sitio web de *The New York Times*. La intervención en la página del periódico, el 13 de septiembre de 1998, fue la primera gran operación hacktivista contra una empresa informativa internacional y evidenció que una nueva generación de hackers estaba pasando de las críticas a la acción directa contra los medios de comunicación tradicionales, a los que consideraban correas de transmisión de gobiernos y empresas. Pero no fue el único embate hacker.

> El ataque contra el sitio del *Times* parece ser la primera vez que los hackers penetran en el sitio web de una organización de noticias importante. Pero los expertos en seguridad informática han señalado que los ataques contra objetivos de alto perfil no son nada raros. Otros objetivos han sido sitios del Pentágono, del Departamento de Justicia, de Coca-Cola, de una filial de Fox TV en Chicago, del Partido Democrático Libre de Alemania y del presidente Ernesto Zedillo de México (Harmon, 1998a)[91].

Los hacktivistas del grupo H4ck1ng 4 G1rl13z (Hacking For Girlies) lograron modificar la página web de *The New York Times* colocando un gran logotipo con sus siglas HFG, ilustrado con imágenes de mujeres desnudas, junto con una proclama que incluía ataques contra el diario y el periodista John Markoff, a quien Kevin Mitnick había acusado de ser el responsable de sus desgracias. El incidente, en clave sarcástica, obligó a suspender la edición electrónica del periódico entre las 10.20 y las 19.30 horas local. A la par, la campaña 'Free Kevin' impulsada por la revista hacker *2600* se desarrolló tanto en circuitos electrónicos como callejeros durante 1998 y 1999, exhibiendo una de las primeras manifestaciones de activismo híbrido.

Ilustración 9: Hackeo de la página web de *The New York Times*, el 13 de septiembre de 1998.

Fuente: http://www.2600.com/hackedphiles/nytimes/hacked/.

La liberación de Mitnick, el 20 de enero del año 2000, se produjo sólo seis días después de que la industria cinematográfica estadounidense interpusiera una demanda

[91] Todas las citas de Harmon (1998a, 1998b) son traducciones propias de los textos originales, en inglés.

contra, entre otros, el editor de *2600*, Emmanuel Goldstein, por difundir en esta revista el programa informático DeCSS (Decoder Content Scramblins System), que permitía visualizar los DVD con licencia privativa bajo el sistema operativo libre GNU/Linux. Las reacciones de la comunidad hacker en ambos casos —ya descritos en esta tesis— fueron el síntoma de un nuevo activismo en red que supuso un salto cualitativo para esta comunidad. A raíz de la demanda contra la revista *2600*, Goldstein escribió en la edición de otoño del año 2000:

> Lo que hemos visto en los últimos meses […] es el enorme crecimiento del activismo en nuestra comunidad. El movimiento 'Free Kevin' nos inició en esta dirección y el caso DeCSS nos dio un verdadero impulso. Esto, a su vez, ha conseguido que muchas más personas se involucren y ayuden a solidificar los lazos entre las comunidades que siempre han estado luchando por las mismas cosas de diferentes maneras. Ya que no podemos contar con los medios de comunicación (la mayoría de ellos son propiedad de las empresas que forman parte de la demanda contra nosotros), tenemos que hacerlo nosotros mismos. Como Jello Biafra[92] expuso durante su discurso de apertura en el H2K[93], debemos «convertirnos en los medios de comunicación» (Goldstein, 2009: 589).

A la vez que la comunidad hacker se fue organizando para defenderse del acoso al que era sometida, muchos hackers empezaron a trascender su *realidad* y a mirar fuera, al mundo que les rodeaba. Ya no bastaba con defender a la comunidad hacker de agresiones institucionales; sus habilidades técnicas debían ser puertas al servicio de causas sociales más generales.

Las acciones políticas más tempranas de los hackers en el ciberespacio se concretaron principalmente en acceder a sitios web para desfigurarlos. Se dice que la primera desfiguración de un sitio web con motivaciones políticas se produjo el 17 de agosto de 1996, cuando un grupo hacker anónimo intervino la página del Departamento de Justicia de Estados Unidos para protestar contra los intentos de la Administración Clinton de regular Internet.

---

92 Jello Biafra (Boulder, Colorado, Estados Unidos, 17 de junio de 1958) es un músico punk y activista político cuyo nombre real es Eric Reed Boucher. Fue cantante y líder de los Dead Kennedys durante la primera etapa de la banda. Es militante del Green Party (Partido Verde), autoproclamado anarquista que aboga por la desobediencia civil y heredero de la tradición activista de los *yippies* sobre cuestiones de derechos humanos, justicia social y anticorporativismo.

93 El H2K fue la tercera conferencia HOPE organizada por la revista *2600*, celebrada entre el 14 y el 16 de julio de 2000 en el Hotel Pennsylvania de Nueva York, con un marcado sesgo activista. Jello Biafra fue el invitado estrella, el 15 de julio de aquel año, para intercambiar ideas, motivaciones y preocupaciones convergentes con la comunidad hacker, tales como el control corporativo de los medios de comunicación, la censura, el futuro de Internet, Napster, las radios piratas, el activismo en línea y la cultura hacker. Se puede consultar más información sobre este evento en: http://www.h2k.net/ (último acceso: 19 de junio de 2015).

El Congreso estadounidense había aprobado el 1 de febrero la Telecommunications Act, que, principalmente, dejaba en manos de las grandes corporaciones de telecomunicaciones el desarrollo y control de las ciberautopistas de la información e introducía una cláusula moral mediante la Communications Decency Act (Ley de Decencia en las Comunicaciones), con la intención de establecer un código de conducta en Internet en Estados Unidos para evitar la presencia en la Red de material que pudiese ser considerado obsceno o indecente, lo cual abría las puertas de par en par a la censura. Clinton firmó la ley el 8 de febrero. Ese mismo día, en respuesta a la Telecommunications Act, John Perry Barlow hizo pública en el Foro Económico Mundial de Davos (Suiza) la *Declaración de Independencia del Ciberespacio*, un manifiesto utópico que llama a la desobediencia y a la ruptura radical entre el ciberespacio y el mundo físico para la auténtica emancipación y soberanía del individuo.

Ilustración 10: Desfiguración de la página web del Departamento de Justicia de Estados Unidos, el 17 de agosto de 1996.

Fuente: http://www.2600.com/hackedphiles/doj/.

Por su radical interés e influencia política en el movimiento ciberactivista, en general, y en el hacktivista, en particular, reproducimos la declaración íntegra de la *Declaración de Independencia del Ciberespacio*, que marca un punto de inflexión en la resistencia contra el control del ciberespacio y en la lucha por el flujo libre de información; un texto que Thierer y Szoka (2009) obervan como "la articulación más temprana (y más extrema)" de una corriente ciberexcepcionalista:

> Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos.
>
> No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquélla con la que la libertad siempre habla. Declaro

el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente.

Los gobiernos derivan sus justos poderes del consentimiento de los que son gobernados. No habéis pedido ni recibido el nuestro. No os hemos invitado. No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece de nuestras acciones colectivas.

No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.

Proclamáis que hay problemas entre nosotros que necesitáis resolver. Usáis esto como una excusa para invadir nuestros límites. Muchos de estos problemas no existen. Donde haya verdaderos conflictos, donde haya errores, los identificaremos y resolvereremos por nuestros propios medios. Estamos creando nuestro propio Contrato Social. Esta autoridad se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente.

El Ciberespacio está formado por transacciones, relaciones y pensamiento en sí mismo, que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos.

Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento.

Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o el conformismo.

Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia. Aquí no hay materia.

Nuestras identidades no tienen cuerpo, así que, a diferencia de vosotros, no podemos obtener orden por coacción física. Creemos que nuestra autoridad emanará de la moral, de un progresista interés propio y del bien común. Nuestras identidades pueden distribuirse a través de muchas jurisdicciones. La única ley que todas nuestras culturas reconocen es la Regla de Oro. Esperamos poder construir nuestras soluciones particulares sobre esa base. Pero no podemos aceptar las soluciones que estáis tratando de imponer.

En Estados Unidos hoy habéis creado una ley, el Acta de Reforma de las Telecomunicaciones, que repudia vuestra propia Constitución e insulta los sueños de Jefferson, Washington, Mill, Madison, DeToqueville y Brandeis. Estos sueños deben renacer ahora en nosotros.

Os atemorizan vuestros propios hijos, ya que ellos son nativos en un mundo donde vosotros siempre seréis inmigrantes. Como les teméis, encomendáis a vuestra burocracia las responsabilidades paternas a las que cobardemente no podéis enfrentaros. En nuestro mundo, todos los sentimientos y expresiones de humanidad, de las más viles a las más angelicales, son parte de un todo único, la conversación global de bits. No podemos separar el aire que asfixia de aquél sobre el que las alas baten.

> En China, Alemania, Francia, Rusia, Singapur, Italia y los Estados Unidos estáis intentando rechazar el virus de la libertad erigiendo puestos de guardia en las fronteras del Ciberespacio. Puede que impidan el contagio durante un pequeño tiempo, pero no funcionarán en un mundo que pronto será cubierto por los medios que transmiten bits.
>
> Vuestras cada vez más obsoletas industrias de la información solían perpetuarse a sí mismas proponiendo leyes, en América y en cualquier parte, que reclamen su posesión de la palabra por todo el mundo. Estas leyes solían declarar que las ideas son otro producto industrial, menos noble que el hierro oxidado. En nuestro mundo, sea lo que sea lo que la mente humana pueda crear, puede ser reproducido y distribuido infinitamente sin ningún coste. El trasvase global de pensamiento ya no necesita ser realizado por vuestras fábricas.
>
> Estas medidas cada vez más hostiles y colonialistas nos colocan en la misma situación en la que estuvieron aquellos amantes de la libertad y la autodeterminación que tuvieron que luchar contra la autoridad de un poder lejano e ignorante. Debemos declarar nuestros «yoes» virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extenderemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos.
>
> Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes.
>
> (Barlow, 1996).

Aquellas palabras de Barlow reverberaron en el ciberespacio. La acción gubernamental fue respondida con una reacción civil que se tradujo en las primeras operaciones hackers aisladas con fines políticos —como la llevada a cabo contra la página web del Departamento de Justicia de Estados Unidos—, pero también en la articulación de nuevos movimientos y organizaciones de ciberderechos y de derechos civiles, de los que surgió la Global Internet Liberty Campaign.

Fundada en junio de 1996, en el marco del encuentro anual de la Internet Society en Montreal (Canadá), la Global Internet Liberty Campaign ha integrado a 68 organizaciones de todo el mundo por las libertades civiles y los derechos humanos. Sus fundadores fueron: American Civil Liberties Union, Association des Utilisateurs d'Internet, CITADEL-EF France, CypherNet, Electronic Frontiers Australia, Electronic Frontier Canada, Electronic Frontier Foundation, EFF-Austin, Electronic Privacy Information Center, Human Rights Watch, Internet Society, NetAction, Peacefire, Privacy International y Quintessenz E-zine. Su objetivo principal ha sido luchar contra la censura previa en las comunicaciones en línea, la defensa de la libertad de expresión y del acceso universal a Internet, la protección de la privacidad de los individuos mediante el cifrado de sus comunicaciones y la lucha contra los

controles restrictivos gubernamentales y corporativos sobre el hardware, el software y la infraestructura de las telecomunicciones. Encabezadas por la American Civil Liberties Union, su primer gran triunfo se produjo en junio de 1997, en el conocido como caso Reno *vs* ACLU, en el que el Tribunal Supremo de Estados Unidos declaró inconstitucional la Communications Decency Act por afectar al derecho de libertad de expresión amparado por la Primera Enmienda.

Ese mismo año, el 10 de febrero, el grupo hacker portugués T0XyN puso en marcha la campaña 'Free East Timor - Free Xanana Gusmão' en defensa de la independencia de Timor Oriental. La operación se ejecutó entre 1997 y 1998, con el apoyo de otros hackers, principalmente el también gupo portugués Pulhas y un hacker catalán conocido como Savage (Molist, 2014). Esta campaña introdujo novedades estratégicas: objetivos múltiples, persistencia y colaboración. El método, sin embargo, fue el tradicional: la desfiguración de sitios web. Su declaración fue la siguiente:

> Esperamos llamar la atención sobre la necesidad de autodeterminación e independencia del pueblo de Timor, oprimido y violado durante décadas por el Gobierno de Indonesia. Esperamos que le des toda tu atención a este paso histórico hacia la libertad, te pedimos que nos ayudes a combatir la tiranía de la ocupación indonesia en Timor (Eurinomo y Quickzero, 2008)[94].

El primer objetivo fue alcanzado el 11 de febrero de 1997: la página web del Departamento de Asuntos Exteriores de la República de Indonesia.

Ilustración 11: Hackeo de la página web del Ministerio de Asuntos de Exteriores indonesio.

Fuente: http://hackstory.net/upload/2/2c/Toxyn2.png.

[94] Traducción propia.

Los hackeos en servidores gubernamentales y comerciales indonesios se sucedieron durante aquel año. En todos ellos, los hacktivistas se preocuparon de no borrar ni destruir nada y de presentar sus acciones como una nueva forma de protesta civil, como afirmaron en sus mensajes en las páginas hackeadas y en el sitio web creado para esta campaña[95]. En casi todos sus hackeos dejaron el siguiente mensaje:

> No hemos destruido ningún servidor. Las páginas originales han sido renombradas. Las páginas principales, historial de archivos y registros han sido alterados para nuestra supervivencia. Las organizaciones de hackers afiliadas y administradores de los sistemas involucrados no deben ser considerados responsables. Somos como otros manifestantes en las calles, pero que simplemente tienen la habilidad de poder acceder a estos sitios. ¡Podéis intentar restringir la información, pero la tecnología nos hace ser a todos iguales! (T0XyN, en http://www.2600.com/hackedphiles/timor011998/indo3/)[96].

Pero hubo una excepción. El 22 de noviembre de 1997, los hackers portugueses tumbaron la página web de la Agencia para la Valoración y la Aplicación de la Tecnología y con ella, otros 27 servidores gubernamentales y comerciales fueron afectados, borrando por primera y única vez los datos de algunas páginas web y desfigurando otras. Para justificar su acción, dejaron este mensaje:

> Este ataque no es contra el pueblo indonesio, sino contra su Gobierno y su opresión a la república de timor [*sic*]. Estas acciones se han realizado para honrar y recordar a las 250 personas asesinadas en Dili el 12 de noviembre de 1991. Como resultado, todos los sitios pertenecientes al gobierno de Indonesia fueron borrados, el resto sólo tenía sus páginas cambiadas. (T0XyN, en http://www.2600.com/hackedphiles/timor010198/indo/)[97].

El 19 de enero de 1998, los hackers portugueses volvieron a desfigurar varios sitios web gubernamentales y comerciales. Un año después, el 30 de agosto de 1999, los ciudadanos de Timor Oriental aprobaron en referéndum su independencia de Indonesia. El 20 de mayo de 2002, Timor Oriental fue proclamado Estado soberano.

---

95 La revista *2600* conserva parte de la página web creada para la campaña en defensa de Timor Oriental y copias de los hackeos, disponibles en:
http://www.2600.com/hackedphiles/east_timor/
http://www.2600.com/hackedphiles/east_timor/them.html.
http://www.2600.com/hackedphiles/timor010198/indo/
http://www.2600.com/hackedphiles/timor011998/indo1/
http://www.2600.com/hackedphiles/timor011998/indo2/
http://www.2600.com/hackedphiles/timor011998/indo3/
[últimos accesos: 15 de mayo de 2015].

96 Traducción propia.

97 Traducción propia.

Otro de los casos más sonados de este tipo de táctica fue el de un hacker británico de 18 años conocido como JF, miembro de uno de los primeros grupos hacktivistas internacionales, milw0rm, cuyo lema es "Poniendo de nuevo el poder en manos del pueblo". El 2 de julio de 1998, JF logró hackear —junto con varios colaboradores anónimos del grupo hacker Ashtray Lumberjacks— los sistemas de la compañía británica de alojamiento web EasySpace para incrustar en alrededor de trescientos sitios web de todo el mundo imágenes y texto antinucleares. La imagen de una nube de hongo nuclear fue acompañada por un texto de unas ochocientas palabras introducido con el siguiente encabezado: "Esta toma de control masiva va para todas las personas ahí fuera que quieren la paz en este mundo" (Wray, 1998; Glave, 1998).

Un mes antes, el 3 de junio, el grupo causó estragos en los servidores de correo electrónico y web del Centro de Investigación Atómica de Bhabha, en India, en protesta por las pruebas nucleares. La revista *Wired* informó que la incursión en los servidores de EasySpace fue, tal vez, "el mayor «hackeo masivo» jamás emprendido" (Glave, 1998). El periódico *Ottawa Citizen* lo describió como "un *hack* de masas sin precedentes" (Paquin, 1998). El artículo firmado por James Glave el 3 de julio de 1998 en *Wired* identifica a los jóvenes miembros de milw0rm como "crackers antinucleares" que habían desfigurado, entre otros, los sitios web de la Copa del Mundo de fútbol, del Campeonato de Wimbledon de tenis, del Ritz Hotel Casino de Londres, de la actriz Drew Barrymore y de la Familia Real saudí. Aquellas no eran acciones anecdóticas, sino las primeras manifestaciones de una nueva forma de activismo facilitado por la Red.

> En ese momento fue el mayor ataque político de su tipo. Desde entonces, y cada vez más en el transcurso del año, hubo numerosos informes de sitios web accedidos por hacktivistas y alterados con contenido político (Wray, 1998).

Cuando se produjeron las más tempranas acciones políticas de hackers en el ciberespacio nadie hablaba aún, al menos públicamente, de hacktivismo. Wray sitúa el surgimiento del hacktivismo con identidad propia en 1998, junto a otro fenómeno similar, el de la desobediencia civil electrónica. Tomados en conjunto, Wray (1998) considera que tanto las acciones de desobediencia civil electrónica más simbólicas como los eventos hacktivistas más tangibles se inscriben en lo que denomina la acción política extraparlamentaria directa en la Red, tomando *extraparlamentario* en el

sentido de la política no electoral o partidista, principalmente la política de base de los movimientos sociales.

En 1998, a la par que los hackers descubrían el potencial político de la Red, el grupo activista Electronic Disturbance Theater, fundado en 1997, agitó y empujó a otros activistas a una nueva experimentación con acciones de desobediencia civil electrónica, dirigidas principalmente contra el Gobierno mexicano y en apoyo a los zapatistas. Sus cofundadores —Stefan Wray, Carmin Karasic, Brett Stalbaum y Ricardo Domínguez— desarrollaron una teoría y práctica de la desobediencia civil electrónica a partir de sus lecturas y observaciones de otros activistas que experimentaban con formas tempranas de sentadas virtuales. El 1 de enero de 1998, inauguraron el año en el que el hacktivismo se dio a conocer al mundo publicando un falso comunicado del subcomandante cibernético Z, del Intercontinental Cyberspace Liberation Army, una organización inexistente. Evidentemente, se trataba de una *broma* de Año Nuevo, pero que contenía una declaración de principios que anticipaba los tiempos hacktivistas. La misiva fue dirigida al presidente mexicano Ernesto Zedillo, al presidente estadounidense Bill Clinton, a los zapatistas y al mundo entero. Fue una declaración de guerra en red contra el Estado mexicano:

> Hace cuatro años, grupos de enmascarados zapatistas, miembros del EZLN [Ejército Zapatista de Liberación Nacional], convergieron y ocuparon militarmente San Cristóbal de Las Casas, en las tierras altas de Chiapas, el Estado más meridional de México. Hoy, bandas de guerreros en red de todo el mundo, miembros del Ejército de Liberación Intercontinental del Ciberespacio, están convergiendo en el ciberespacio para instigar la guerra de información, la guerra en red, contra el Gobierno mexicano cotrolado por el PRI.
>
> La masacre de Acteal del 22 de diciembre de 1997 es la gota que ha colmado el vaso. ¡Ya basta! Ya no vamos a quedarnos de brazos cruzados ante nuestras pantallas de ordenador. No vamos a esperar más ni a pensar estúpidamente que la justicia prevalecerá por su propio acuerdo. La justicia únicamente prevalecerá a través de la lucha. Y nosotros, los guerreros en red del Ejército de Liberación Intercontinental del Ciberespacio, estamos listos para lanzar un ataque coordinado.
>
> En respuesta al asalto paramilitar del PRI en Chenalhó apoyamos lo siguiente:
>
> - Aislamiento del Gobierno mexicano en la comunidad internacional.
> - Interferencia coordinada y obstrucción de las redes digitales de México.
> - Desestabilización de la infraestructura de telecomunicaciones de México.
> - Destrucción virtual de la presencia corporativa de Estados Unidos en México.
> - Acción global unificada para forzar la discusión sobre atrocidades recientes.

> Tenemos la capacidad técnica para poner al Gobierno de rodillas.
>
> El Ejército de Liberación Intercontinental del Ciberespacio tiene a su disposición algunas de las mejores mentes en computación. Estamos listos y dispuestos a hacer nuestro trabajo.
>
> ¡Muerte al PRI!
>
> ¡Viva las [*sic*] Zapatistas!
>
> Desde la región montañosa del centro de Texas, el subcyber-comandante Z.
>
> Ejército de Liberación Intercontinental del Ciberespacio.
>
> (Electronic Disturbance Theater, 1998)[98].

A lo largo de 1998, el Electronic Disturbance Theater desarrolló, ejecutó e hizo accesible para su descarga en su página web[99] un software llamado FloodNet, creado por la programadora y artista multimedia Carmin Karasic y por Brett Stalbaum, teórico investigador en información, bases de datos y desarrollo de software. FloodNet es un *applet* de Java[100] que permite a muchos usuarios, en un momento determinado, golpear masivamente un servidor escogido como blanco. El *applet* está programado para que repetida y constantemente se carguen cada x segundos una serie de páginas elegidas como objetivos, hasta que el servidor se caiga por saturación. La colectividad de la acción es imprescindible para que ésta tenga éxito. Floodnet fue ejecutado en distintas ocasiones en apoyo a los zapatistas: el 10 de mayo, el 10 de junio, el 28 de junio, el 3 de julio y el 19 de julio. Pero fue el 9 de septiembre cuando el Electronic Disturbance Theater ejecutó la primera gran operación hacktivista de la historia.

La acción se desarrolló durante la celebración del Ars Electronica Festival[101], en Liz, Austria, que aquel año se dedicó a las infoguerras. La organización exhibió allí su proyecto *SWARM* (enjambre) y ejecutó un ataque masivo con FloodNet a tres bandas, dirigido contra un objetivo político, otro militar y un tercero económico: los sitios web de la Presidencia de México, el Pentágono y la Bolsa de Frankfurt. Con esta acción, los hacktivistas querían manifestar su apoyo a los zapatistas y su oposición al

---

98 Traducción propia.

99 El sitio web del Electronic Disturbance Theater dedicado a la desobediencia civil electrónica aún puede visitarse en esta URL: http://www.thing.net/~rdom/ecd/ecd.html (último acceso: 24 de septiembre de 2015). Su última actualización data del 19 de marzo de 2008.

100 Un *applet* es un componente de software escrito en un lenguaje de programación que se ejecuta bajo el control de una aplicación mayor que lo contiene, por ejemplo, un navegador web. Un *applet* Java está escrito en lenguaje Java, orientado a objetos, es decir, se basa en dividir el programa en pequeñas unidades lógicas de código llamadas objetos que interactúan entre sí mediante mensajes.

101 Ars Electronica, con sede en la ciudad austriaca de Linz, es una organización fundada en 1979 que premia cada año, desde 1987, los mejores y más vanguardistas proyectos de arte electrónico y digital de todo el mundo en siete categorías.

Gobierno mexicano, al Ejército de Estados Unidos y a la economía neoliberal global. FloodNet fue inutilizado en una acción a la contra del Departamento de Defensa estadounidense, que había diseñado un *applet* de Java hostil a FloodNet.

Unas veinte mil personas en todo el mundo se conectaron a FloodNet entre el 9 y el 10 de septiembre, pero sus golpes a los servidores no fueron suficientes para tumbarlos. El *applet* hostil generó serios problemas en los discos duros de los ciberactivistas e incluso obligó a muchos a reiniciar sus ordenadores. Al mismo tiempo, Wray —por entonces, doctorando— recibió un mensaje de correo electrónico de la New York University en el que se le informaba de que la Agencia de Sistemas de Información para la Defensa de Estados Unidos se había quejado de contenido publicado por Wray sobre desobediencia civil electrónica, alojado en los servidores de la institución académica; finalmente, fue retirado.

La acción del Electronic Disturbance Theater resultó un fiasco técnico, pero fue una victoria simbólica, ya que primero resonó en los medios europeos, más tarde se hicieron eco de ella medios especializados estadounidenses como la revista *Wired*, el canal de televisión ZDTV o el periódico semanal *Defense News*, además de la red de estaciones National Public Radio, entre otros, y, finalmente, el hacktivismo saltó a la prensa generalista. Wray señala además la aparición aquel año de los primeros informes sobre hacktivismo en países como Reino Unido, Australia, India o China.

II.5.3. Primeras referencias al hacktivismo en los medios de masas

1998 fue el año del salto del hacktivismo a los medios de comunicación de masas. El *Ottawa Citizen* fue uno de los primeros medios convencionales en ofrecer una descripción en profundidad de los hacktivistas. El 26 de octubre, el periodista Bob Paquin introdujo el término *hacktivista* en un amplio artículo publicado en este periódico con el título ‘E-Guerrillas in the mist’. Paquin es uno de los primeros periodistas en describir al gran público el salto del *hacking* al hacktivismo, la materialización de código informático en acción política.

> Las primeras generaciones de hackers se deleitaban con el reto de explorar electrónicamente la geografía digital del nuevo paisaje que se creó a través de la revolución de la computadora. […] Sin embargo, una segunda generación ha saltado a la palestra. Los llamados hacktivistas se dedican al ciberactivismo, o lo que algunos han llamado hacking ético (Paquin, 1998).

En este artículo, el periodista describe algunas de las primeras acciones hacktivistas, entre las que recoge la del grupo mexicano X-Ploit, que en agosto de aquel año hackeó el sitio web del Ministerio de Finanzas de su país e incrustó la cara del héroe revolucionario Emiliano Zapata, en solidaridad con la rebelión zapatista en Chiapas; la del grupo portugués Kaotik, cuando hackeó el 1 de agosto cuarenta y cinco sitios web del Gobierno de Indonesia para ocuparlos con mensajes de apoyo a la plena autonomía de Timor Oriental; los *mailbombs* enviados y sitios web hackeados el 12 de agosto por hackers de China y Taiwán para protestar contra la tortura, violación y saqueos que ciudadanos chino-indonesios sufrieron durante los disturbios contra el derrocado tirano indonesio Suharto en mayo de aquel año; el hackeo de la página web de *The New York Times* el 13 de septiembre, o la incursión de hacktivistas en un sitio web del Gobierno de India, el 13 de octubre, para incrustar imágenes y textos contra la represión y violación de derechos humanos en la región de Cachemira.

Una de las fuentes de Paquin fue Wray, quien le describió de esta manera la emergencia del hacktivismo:

> Aunque los hackers non son claramente contrarios a transgredir el límite entre lo legal y lo ilegal, no todos los hackers son políticos. Pero hoy, el hacker politizado es claramente un subgrupo creciente en el mundo hacker (Wray, en Paquin, 1998)

El clima hacktivista iba penetrando poco a poco en la esfera pública y sus acciones ya eran vistas en sus primeras manifestaciones como actos políticos. Wray continúa explicando:

> Uno a uno, los sitios web más destacados del mundo están cayendo por las balas cibernéticas de hackers de Internet. A diferencia del pasado, la nueva generación de intrusos electrónicos tiene una agenda política (Wray, en Paquin, 1998).

El 31 de octubre de 1998, el Electronic Disturbance Theater apareció en la primera página de *The New York Times*, citado junto con otros grupos hacktivistas que estaban emergiendo por entonces. El artículo, firmado por la periodista Amy Harmon con el título '«Hacktivists» of All Persuasions Take Their Struggle to the Web'[102], es el primer registro en el tiempo que se encuentra en el buscador del sitio web del periódico estadounidense para las palabras *hacktivismo* y *hacktivistas*.

[102] Obsérvese el uso de comillas de *The New York Times* para marcar un neologismo que por entonces era desconocido para el gran público y que se estaba estrenando en los medios de comunicación.

Ilustración 12: Portada de *The New York Times* del 31 de octubre de 1998.


The New York Times

Middle Ground Is Good Ground, 2 Candidates in California Find

Democrats Gain by Portraying Foes as Extremists

ECONOMIC GROWTH SURPRISINGLY SOLID IN THIRD QUARTER

42d St. Revival May Alter Face Of Theater Row

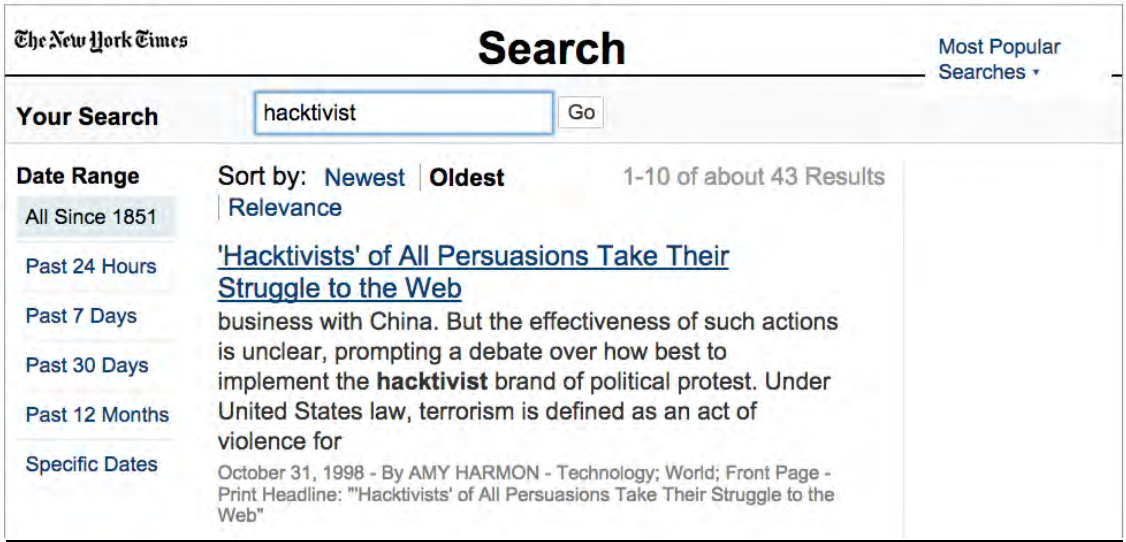
Wealthy Nations Back Plan To Speed Help to the Weak

Political Wives Cast as Leads In TV Testimonials for Votes

'Hacktivists' of All Persuasions Take Their Struggle to the Web

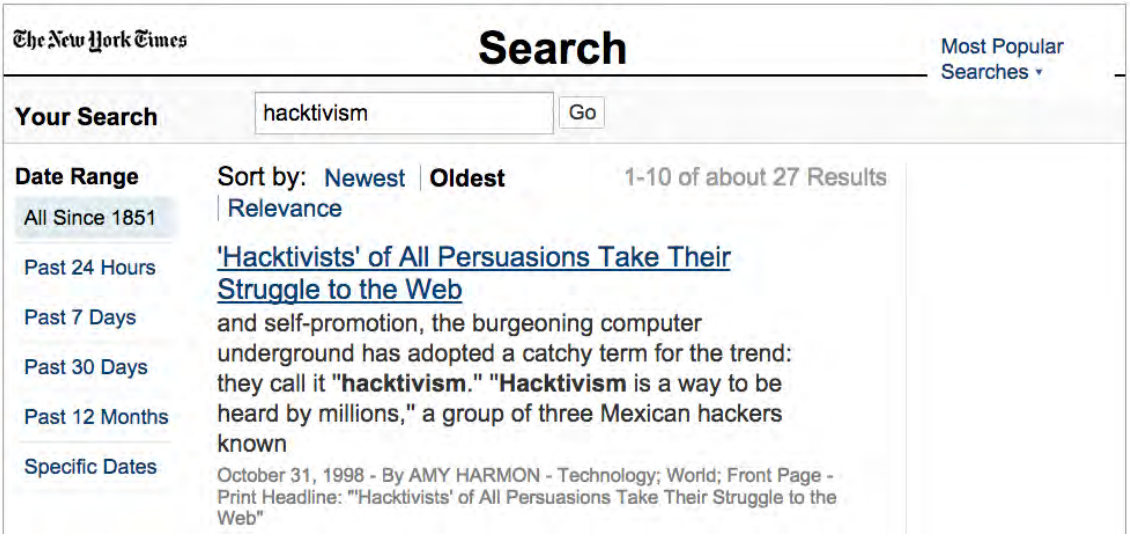
Fuente: *The New York Times* (titular recuadrado por el autor de esta tesis).

Ilustración 13: Entrada más antigua en el buscador en línea de *The New York Times* con la palabra *hacktivist*.



Fuente: captura propia tomada del buscador *online* de *The New York Times*.

Ilustración 14: Entrada más antigua en el buscador en línea de *The New York Times* con la palabra *hacktivism*.



Fuente: captura propia tomada del buscador *online* de *The New York Times*.

The New York Times fue el primer medio global que introdujo a las masas en el *conocimiento* del hacktivismo. Lo más interesante de este artículo, además de la presentación de los neologismos *hacktivismo* y *netwar*, es la distinción que Harmon establece entre lo que llama "activistas y hackers radicales", dos "subculturas subversivas distintas que rara vez se han cruzado" pero que han encontrado en la desobediencia civil electrónica el imán que une "dos psicologías" que "de alguna manera son polos opuestos" (Harmon, 1998b)[103]. La periodista advierte que, hasta entonces, los activistas habían prestado poca atención a la infraestructura de la información sobre la que descansa la estructura de poder. Al contrario, los hackers ya habían definido claramente la relación entre poder e información guiados por el adagio "La información quiere ser libre", un mantra que

> refleja la creencia de que, como las tecnologías de la información son más baratas y accesibles, quienes intentan limitar y controlar el flujo de información lo tendrán cada vez más difícil y la información se resistirá al impedimento, a la restricción y a la obstrucción (Jurgenson y Rey, 2014: 2651).

La tradicional criminalización del hacker emerge, una vez más, en el discurso mediático. La periodista de *The New York Times* los describe como individuos "antiautoritarios", "enamorados de su imagen de vaqueros de la frontera electrónica" y

[103] Todas las citas tomadas de Harmon son traducciones propias del texto original, en inglés.

que sólo han cometido "actos de vandalismo sin sentido" y "robado el número de alguna tarjeta de crédito". También explica que "el rápido crecimiento de Internet ha transformado lo que antes era un parque de hackers en, entre otras cosas, una plataforma política de largo alcance" (Harmon, 1998b). Pero lo que es más interesante:

> Los grupos radicales están descubriendo lo que los hackers han sabido siempre: las instituciones sociales tradicionales son más vulnerables en el ciberespacio que en el mundo físico. Y algunos miembros del famosamente inmaduro *underground* hacker están siendo motivados por causas distintas a la gratificación del ego (Harmon, 1998b).

Harmon reporta acciones hacktivistas ejecutadas por grupos dispares y desde distintas partes del mundo: sitios web de los gobiernos de China e India intervenidos en defensa de los derechos humanos, contra los abusos de poder en estos países y contra las pruebas nucleares indias; o la toma de sitios web indonesios contra los atropellos en Timor Oriental.

En esta primera erupción hacktivista, la naturaleza y objetivos de las acciones eran tan variados como sus actores. Organizaciones en defensa de los derechos de los animales como Animal Liberation Front, libertarios de las comunicaciones como Radio4All o adolescentes antiimperialistas organizados en red con seudónimos cibernéticos participaron en estas primeras expresiones hacktivistas.

Para entonces, el concepto *netwar* propuesto por los analistas de RAND ya había calado y las acciones del Electronic Disturbance Theater hacían emerger el aforismo "La revolución será digitaliza".

> Hasta que declararon la «guerra en red» contra el Gobierno de México, Ricardo Domínguez y Stefan Wray consiguieron sus credenciales como activistas a la vieja usanza, asistiendo a mítines en apoyo a los rebeldes zapatistas, repartiendo panfletos, gritando consignas políticas. Ahora, los dos neoyorquinos organizan «sentadas virtuales» y reclutan programadores informáticos para atacar sitios de la World Wide Web de cualquier persona o empresa que consideren responsables de actos de opresión. Su nuevo grito de guerra: «La revolución será digitalizada» (Harmon, 1998b).

II.5.4. Hacktivismo por los derechos humanos

Las acciones de desobediencia civil electrónica de activistas informatizados siguieron sucediéndose en 1998, con el Electronic Disturbance Theater como principal

actor. El 22 de noviembre, este colectivo ejecutó otra acción mediante FloodNet contra la US Army School of the Americas[104], un centro operado por el Departamento de Defensa de Estados Unidos para la formación militar, conocido por haber formado en métodos de tortura, asesinato y represión a militares y policías de toda Latinoamérica. Por último, como gran acto final de la primera temporada hacktivista, el Electronic Disturbance Theater lanzó al ciberpesacio una versión pública descargable de FloodNet a las 00.01 horas del 1 de enero de 1999.

Todas estas primeras ciberacciones de activistas digitalizados y hackers activistas que Wray enmarca, en su conjunto, como formas de hacktivismo, pudieron verse entre los veteranos hackers más ortodoxos como una transgresión de la ética hacker. De hecho, algunos hackers que participaron en el Ars Electronica de Linz dedicaron duras críticas a FloodNet por considerarla una ciberarma cuyo uso supone "un abuso inaceptable de la Red" (Electronic Disturbance Theater, 1998b). Sin embargo, en el caso de las acciones ejecutadas por el grupo hacktivista milw0rm, John Vranesevich, fundador del sitio web Antionline.com sobre seguridad informática, constató que "de los miles de correos electrónicos" que habían conseguido sobre milw0rm, en "el 97,3 por ciento de ellos se pensaba que sus miembros eran héroes, con menos del tres por ciento pensando en ellos como criminales" (Paquin, 1998).

Las tensiones entre la vanguardia hacker más *ética* y los grupos más radicalizados se evidenciaron y agudizaron aún más en 1999, cuando las publicaciones estadounidenses *2600* y *Phrack*, el Chaos Computer Club alemán, la organización Cult of the Dead Cow radicada en Lubbok (Texas), el colectivo español !Hispahack, el grupo L0pht Heavy Indusries de Boston (Massachusetts), los grupos portugueses Pulhas y T0xyn, y diversos hackers holandeses, incluido el experto en criptografía Rop Gonggrijp, emitieron un comunicado conjunto el 7 de enero para rechazar la declaración de ciberguerra de un grupo estadounidense denominado Legion of the Underground contra Irak y China, motivada por los abusos de los derechos humanos en estos países.

Legion of the Underground no era un grupo formado por novicios; llevaba operando unos siete años y entre la veintena de miembros de este colectivo se hallaban

[104] Este centro, creado en 1946, fue rebautizado en 2001 como Western Hemisphere Institute for Security Cooperation.

algunos hackers especialmente habilidosos, incluido un programador que se había formado en el Ejército de Estados Unidos y que poseía amplios conocimientos sobre seguridad de redes (Ruffin, 2004). El grupo se estaba preparando para interrumpir las redes de comunicación chinas e iraquíes. Su anuncio hizo reaccionar a los más notables grupos internacionales de hackers, contrarios a estas prácticas por suponer una transgresión de la ética de esta comunidad.

La declaración de la autodenominada Coalición Internacional de Hackers fue un llamamiento a los hacktivistas de todo el mundo para que rechazasen cualquier intento de dañar las infraestructuras de información y comunicación de cualquier país. Aunque las versiones en inglés y en español de este comunicado difieren en algunos párrafos, ambas exponen los mismos argumentos. Por su interés, reproducimos íntegro el texto publicado por el grupo !Hispahack:

> Los grupos de hackers 2600, Chaos Computer Club, The Cult of the Dead Cow (cDc), !Hispahack, L0pht Heavy Industries, Phrack, Pulhas y T0xyn sienten la necesidad de comentar el reciente anuncio de un grupo que se hace llamar «Legion of the Underground» (LoU).
>
> LoU ha declarado que trataran [*sic*] de dañar y sabotear la infraestructura del ciberespacio de Iraq y China. Citan los problemas con los derechos humanos en esos países como la causa de esta acción.
>
> Aunque podamos estar de acuerdo con LoU en que las atrocidades en China e Iraq deben terminar, estamos en desacuerdo con los métodos que propugnan. Estos son cortos de miras y potencialmente contraproducentes. No se puede esperar legítimamente mejorar el libre acceso de un país a la información tratando de inhabilitar sus redes de datos.
>
> Sin duda, la situación de los derechos humanos en China, Iraq y muchos otros países de este planeta es pésima. El Hacktivismo —usar las habilidades y herramientas de hacking para apoyar causas progresistas— puede ser en algunos casos, a ojos de algunos de los abajo firmantes, una manera legítima de atraer la atención pública a estos problemas.
>
> Pero nos oponemos totalmente a cualquier intento de usar el poder del hacking para amenazar o destruir las infraestructuras de comunicación de cualquier país, por ninguna razón. Declarar la «guerra» contra alguien, cualquier grupo de personas o nación es un acto totalmente deplorable. Lo único que hace es reducir al hacker al mismo nivel del grupo o país que está atacando. Esto no tiene ninguna relación con el hacktivismo o las éticas del hacker, y no es nada de lo que ningún hacker deba sentirse orgulloso.
>
> Los gobiernos de todo el mundo están intentando establecer el ciberespacio como el nuevo campo de guerra para sus conflictos artificiales. Lo que LoU ha hecho es legitimar inadvertidamente estos propósitos. Si los hackers se establecen como armas, el hacking en general se verá como una acción de guerra. Y los mismos hackers serán vistos, sin ninguna duda, como objetivos legítimos para los países contendientes.

> Desde nuestro punto de vista, LoU está haciendo cosas que los gobiernos del mundo no quieren hacer pública u oficialmente. Los preparativos para la «Guerra de la Información» están, en los EE.UU. y en cualquier otra parte, en un punto en que son necesarios casos «reales» para justificar los fondos asignados.
>
> LoU está proporcionando ahora este caso real. Creemos que LoU debería investigar cuidadosamente si la idea de declarar la «guerra» a China e Iraq no fue dada por alguien con intereses distintos a los de defender el problema de los derechos humanos.
>
> Los firmantes piden a todos los hackers del planeta que rechacen todo aquello relacionado con dañar las infraestructuras de información de cualquier país. No deis soporte a NINGÚN acto de «Ciberguerra»; mantened las redes de comunicaciones vivas: son el sistema nervioso de nuestro planeta. (*LoU Strike Out with International Coalition of Hackers*, 1999)

Lo más sustancial de esta declaración es el reconocimiento que se hace del hacktivismo como manifestación política del *hacking* en favor del progreso de la humanidad, la defensa de la ética hacker como su eje y la desvinculación del hacktivismo de cualquier forma de ciberguerra. Tras su publicación, Legion of the Underground decidió suspender su campaña y se evitó así "lo que fácilmente podría haber causado un incidente internacional" (Ruffin, 2004). Pero la declaración sirvió además para intentar poner ciertos límites a las tácticas hacktivistas.

Tras intercambiar impresiones con Reid Fleming, de Cult of the Dead Cow, y Frank Rieger, del Chaos Computer Club, Ruffin formuló algunas reglas básicas para el hacktivismo. La primera, no ejecutar desfiguraciones web. En su opinión, estas acciones violan el derecho a distribuir información y, por lo tanto, atentan contra la libre expresión de cualquier individuo o grupo legítimamente facultado para publicar contenidos en la Web. En segundo lugar, tampoco ejectutar ataques de denegación de servicio (DDoS), pues entiende que "no hay una gran diferencia entre desactivar la capacidad de un servidor Web para proporcionar información —incluso si esa información es repugnante— y hacer callar a alguien en el pleno de un ayuntamiento" (Ruffin, 2004). Para la corriente más ortodoxa de los hackers activistas, este tipo de prácticas no deben ser identificadas como hacktivismo, sino como acciones de desobediencia digital. Esto supone no sólo un cuestionamiento de las prácticas de los grupos de hackers más radicalizados, sino también de las proclamas y acciones de los grupos activistas digitalizados que se inspiran en las clásicas formas de desobediencia civil y que se autodenominan hacktivistas, como el Electronic Disturbance Theater. La ética hacker traza, para los ortodoxos, la delgada línea que separa el hacktivismo de

otras expresiones ciberactivistas.

Sin embargo, no existe en toda la comunidad hacker un rechazo frontal a algunas de las tácticas hacktivistas más reactivas, mientras no deriven en actos de ciberguerra. Goldstein contradice así a Ruffin en un matiz importante:

> Mientras que hackear una página web de vez en cuando es algo que incluso se puede considerar un gesto de libertad de expresión, las declaraciones de guerra y los intentos de causar daños reales son algo muy diferente, ciertamente (Goldstein: 2009: 261).

El interés de Ruffin en el uso ético de la tecnología y del *hacking* al servicio de los derechos humanos le llevó a fundar en 1999 el grupo internacional Hacktivismo, auspiciado por Cult of the Dead Cow y participado por hackers, activistas de derechos humanos, juristas y artistas interesados en la seguridad informática desde una perspectiva activista. Hacktivismo se creó principalmente para la creación de tecnología anticensura y la promoción de los derechos humanos en Internet, incluidos la privacidad y el acceso a la información como derechos universales. El grupo asumió como punto de partida ético los principios consagrados en la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. Además, apoya a los movimientos de software libre y de código abierto, y se reconoce como una organización sin ánimo de lucro y opuesta al capitalismo tecnológico. Su principal misión ha sido investigar y publicar los resultados de sus trabajos en áreas de tecnologías de la información, comunicación y medios electrónicos, así como asistir, en lo posible, a organizaciones no gubernamentales, grupos de justicia social y entidades de derechos humanos en el uso de tecnologías avanzadas de la información y en el fomento y promoción de sus trabajos. Todo ello, intentando divertirse, como *mandan* los cánones hackers (Hacktivismo, 2004).

El proyecto ha contado con el asesoramiento de Patrick Ball y Cindy Cohn. Ball ha sido director adjunto del Science and Human Rights Program de la American Association for the Advancement of Science[105] y, posteriormente, director ejecutivo

[105] La Asociación Estadounidense para el Avance de la Ciencia (*American Association for the Advancement of Science* - AAAS) es una organización creada en 1848 que promueve el diálogo científico y la cooperación entre científicos, defiende la libertad científica, fomenta la responsabilidad científica y apoya la educación científica para beneficiar a toda la humanidad. En la actualidad es la sociedad científica más grande del mundo. También edita la publicación científica *Science*.

del Human Rights Data Analysis Group[106]. Cohn, por su parte, ha sido directora jurídica de la Electronic Frontier Foundation desde el año 2000 hasta su nombramiento como directora ejecutiva, en 2015.

El 4 de julio de 2001, Cult of the Dead Cow y Hacktivismo publicaron *La Declaración del Hacktivismo*, que incluye un conjunto de reivindicaciones para una Internet libre y sin censura. Por su apreciable interés, reproducimos a continuación el texto original, disponible en la página web del grupo en once idiomas: inglés, chino, francés, alemán, holandés, ruso, húngaro, italiano, portugués, serbio y español[107]:

> PROFUNDAMENTE ALARMADOS porque la censura de la Internet patrocinada por los gobiernos se está diseminando rápidamente con la asistencia de las corporaciones transnacionales,
>
> TOMANDO COMO BASE los principios y propósitos consagrados en el Artículo 19 de la Declaración Universal de los Derechos Humanos (UDHR [Universal Declaration of Human Rights]) que declara que, «Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye la libertad de sostener opiniones sin interferencia y a buscar, recibir e impartir información e ideas a través de cualquier medio y sin consideración de fronteras», y el Artículo 19 del Convenio Internacional sobre los Derechos Civiles y Politicos (ICCPR [International Covenant on Civil and Political Rights]) que afirma,
>
> 1. Todo individuo tendrá el derecho de sostener opiniones sin interferencia.
> 2. Todo individuo tendrá el derecho a la libertad de expresión; este derecho incluirá el derecho a buscar, recibir e impartir información e ideas de todo tipo, sin consideración de fronteras, tanto por medio oral, escrito o impreso, en forma de arte o por cualquier otro medio de su elección.
> 3. El ejercicio de los derechos provistos en el párrafo 2 de este artículo conlleva tareas y responsabilidades especiales. Por lo tanto puede estar sujeto a ciertas restricciones, pero éstas solamente deberán ser tal como están provistas por la ley y son necesarias:
>   a. Por respeto a los derechos o reputación de otros.
>   b. Por la protección de la seguridad nacional o el orden público, o de la salud o moral pública.
>
> RECORDANDO que algunos estados miembros de las Naciones Unidas han firmado el ICCPR, o lo han ratificado en tal manera que impide a sus ciudadanos usarlo en cortes legales,
>
> CONSIDERANDO que tales estados miembros continúan suprimiendo voluntariamente el acceso libre y abierto a la información publicada legalmente en Internet, a pesar de las nítidas palabras del ICCPR al referirse a que la libertad de expresión se extiende a todos los medios de comunicación,

106 El Human Rights Data Analysis Group es una organización no gubernamental y sin ánimo de lucro que aplica métodos científicos para el análisis de violaciones de derechos humanos en todo el mundo. Fue fundada por Patrick Ball en el año 2002 como parte del Science and Human Rights Program y en la actualidad actúa como organización independiente.

107 Se ha respetado el uso de mayúsculas del texto original como recurso exclamativo y apelativo propio de la escritura web.

TOMANDO NOTA de que las corporaciones transnacionales continúan vendiendo tecnologías de la información a los regímenes más represivos del mundo con pleno conocimiento de que lo usarán para rastrear y controlar a una ciudadanía ya bastante hostigada,

TOMANDO EN CUENTA que la Internet se está convirtiendo rápidamente en un medio de represión en vez de un instrumento de liberación,

TENIENDO EN MENTE que en algunos países es un crímen reclamar el derecho de acceder a la información publicada legalmente, y otros derechos humanos básicos,

RECORDANDO que los estados miembros de las Naciones Unidas han fallado al presionar a los más distinguidos violadores de los derechos de la información hacia un estándar más elevado,

CONSCIENTES de que negar el acceso a la información podría conducir a un deterioro espiritual, intelectual y económico, promover la xenofobia y la desestabilización del orden internacional,

PREOCUPADOS porque los gobiernos y las transnacionales se entienden para mantener el statu quo,

PROFUNDAMENTE ALARMADOS porque los líderes mundiales han fallado al tratar el asunto de los derechos de la información de manera directa y sin equívocos,

RECONOCIENDO la importancia de luchar contra los abusos a los derechos humanos con respecto al acceso razonable a la información disponible en la Internet,

POR LO TANTO ESTAMOS CONVENCIDOS de que la comunidad hacker tiene el imperativo moral de reaccionar, y entonces

DECLARAMOS:

QUE EL RESPETO TOTAL POR LOS DERECHOS HUMANOS Y LAS LIBERTADES FUNDAMENTALES INCLUYE LA LIBERTAD DEL ACCESO EQUITATIVO Y RAZONABLE A LA INFORMACIÓN, SEA POR RADIO DE ONDA CORTA, CORREO AEREO [*sic*], TELEFONÍA SIMPLE, LA INTERNET GLOBAL O CUALQUIER OTRO MEDIO.

QUE RECONOCEMOS EL DERECHO DE LOS GOBIERNOS A PROHIBIR LA PUBLICACIÓN DE CIERTOS SECRETOS DE ESTADO OPORTUNAMENTE CATEGORIZADOS, PORNOGRAFÍA INFANTIL, Y ASUNTOS RELACIONADOS CON LA VIDA PRIVADA Y LOS PRIVILEGIOS PERSONALES, ENTRE OTRAS RESTRICCIONES ACEPTADAS. PERO NOS OPONEMOS AL USO DEL PODER DEL ESTADO PARA CONTROLAR EL ACCESO A LOS TRABAJOS DE LAS FIGURAS CRÍTICAS, INTELECTUALES, ARTÍSTICAS Y RELIGIOSAS.

QUE LA CENSURA DE LA INTERNET RESPALDADA POR EL ESTADO EROSIONA LA COEXISTENCIA PACÍFICA Y CIVILIZADA, AFECTA AL EJERCICIO DE LA DEMOCRACIA Y PONE EN PELIGRO EL DESARROLLO SOCIOECONÓMICO DE LAS NACIONES.

QUE LA CENSURA DE LA INTERNET APOYADA POR EL ESTADO ES UNA SEVERA FORMA DE VIOLENCIA ORGANIZADA Y SISTEMÁTICA CONTRA LOS CIUDADANOS, DESTINADA A GENERAR CONFUSIÓN Y XENOFOBIA, Y ES UNA CONDENABLE VIOLACIÓN DE LA CONFIANZA.

> QUE ESTUDIAREMOS LAS FORMAS Y MANERAS DE BURLAR LA CENSURA DE LA INTERNET RESPALDADA POR LOS ESTADOS Y QUE IMPLEMENTAREMOS TECNOLOGÍAS PARA DESAFIAR LAS VIOLACIONES DE LOS DERECHOS A LA INFORMACIÓN.
>
> (Hacktivismo y Cult of the Dead Cow, 2001).

Sobre esta base, Hacktivismo desarrolló y liberó software político para garantizar los derechos y libertades de individuos, especialmente en países donde son reprimidos. Estos fueron sus principales proyectos:

- Torpark: navegador web portátil basado en Firefox y que utiliza la red TOR (The Onion Router), que aplica tecnología criptográfica para proporcionar una navegación anónima y segura. Se ofrece preconfigurado, no requiere instalación, puede funcionar con un dispositivo de memoria USB y no deja huellas en el navegador o computadora del usuario.
- ScatterChat: cliente de mensajería instantánea diseñado para usuarios sin grandes destrezas técnicas que requieren comunicaciones privadas y anónimas, y transferencias de archivos seguras. Especialmente destinado para usuarios finales implicados en la defensa de los derechos humanos y de la democracia que operan en territorios hostiles. ScatterChat es también una valiosa herramienta para cualquier persona que requiera comunicaciones seguras.
- Six/Four: sistema contra la censura basado en un protocolo *peer-to-peer*, redes privadas virtuales, proxies abiertos y esteganografía, que permite engañar a los cortafuegos, habilita túneles seguros de comunicación directa y proporciona a sus usuarios acceso anónimo y seguro a información en la Red. Su nombre es un recuerdo a la fecha de la masacre en Tiananmen, el 4 de junio de 1989.
- Camera/Shy: aplicación anticensura que usa técnicas esteganográficas LSB (Least Significant Bit) y cifrado AES-256 bits que permite compartir información oculta en imágenes en formato gif, protegidas por contraseña y publicadas en algún sitio web. La aplicación es un

> navegador web basado en Internet Explorer que escanea y descifra la información oculta directamente desde la web, sin dejar rastros en el sistema del usuario. Especialmente indicada para activistas que operan tras cortafuegos nacionales. El lanzamiento de esta aplicación se dedicó a la memoria del escritor y disidente chino Wang Ruowang.

Otra de las aportaciones más sustanciales del colectivo Hacktivismo ha sido su licencia HESSLA (Hacktivismo Enhanced-Source Software License Agreement) para liberar su software y promover los objetivos políticos intrínsecos a sus programas informáticos, vinculados a la defensa de los derechos humanos y la libertad y dignidad humana en todo el mundo. HESSLA es una licencia con ciertas restricciones para salvaguardar su uso ético y proteger a sus usuarios finales, generalmente disidentes en regímenes totalitarios. La licencia permite tanto a Hacktivismo como a los usuarios finales de su software acudir a los tribunales si alguien intenta utilizarlo de forma maliciosa o introducir cambios perjudiciales en el software. Por ejemplo, HESSLA prohíbe explícitamente introducir *spyware*, tecnología de vigilancia o cualquier otro código no deseado en las versiones modificadas de los programas bajo esta licencia. Además, la licencia prohíbe cualquier uso del software por cualquier gobierno que viole los derechos humanos y faculta a cualquier usuario final —no sólo a Hacktivismo— a iniciar demandas contra quien use el software con licencia HESSLA con fines abusivos (Ruffin, 2004).

Esta *spin-off* de Cult of the Dead Cow nos introduce en el hacktivismo informacional del siglo XXI, maximizado por WikiLeaks, que ha convivido y se ha complementado en tiempos de emergencia con el hacktivismo reactivo de nuevos actores antisistema, cuyo máximo exponente es Anonymous.

II.6. HACKTIVISMO INFORMACIONAL: NUEVOS RETOS Y DESAFÍOS EN LA ERA DE LA VIGILANCIA GLOBAL

El hacktivismo en el siglo XXI se centra fundamentalmente en la lucha por la transparencia de gobiernos y empresas, y contra el Estado de secreto y su sistema de vigilancia y control masivos mediado por las tecnologías digitales y las redes de comunicación globales.

En el invierno de 1998-1999, en plena eclosión del hacktivismo, Goldstein ya vaticinó una nueva era en el activismo hacker y un nuevo paradigma:

> En los próximos años, vamos a presenciar algunos hitos en el desarrollo humano en relación con la libertad de expresión, comunicaciones, acceso y privacidad. Será el equivalente del movimiento de los derechos civiles, la Revolución Americana y el Siglo de las Luces, todo mezclado (Goldstein, 2009: 269).

Los vaticinios de nuevas revoluciones sociales contra el imperio corportativo-gubernamental no se han circunscrito al mundo hacker. Hace tres lustros, Naomi Klein planteó una hipótesis que hoy vemos parcialmente confirmada en los fenómenos sociales y mediáticos que han originado las filtraciones de secretos gubernamentales y corporativos por parte de WikiLeaks:

> […] a medida que los secretos que yacen detrás de la red mundial de las marcas sean conocidos por una cantidad mayor de personas, su exasperación provocará la gran conmoción política del futuro, que consistirá en una vasta ola de rechazo frontal a las empresas transnacionales, y especialmente aquellas cuyas marcas son más conocidas (Klein, 2001: 24).

La libertad de expresión, la libre comunicación y el acceso libre al conocimiento en el ciberespacio, y la capacidad de controlar y moldear la tecnología para satisfacer nuestras necesidades individuales (Goldstein, 2009: 594), se convirtieron desde la década de 1990 en las principales causas del incipiente activismo hacker. A estas preocupaciones se sumaron el afán por la transparencia en gobiernos y corporaciones empresariales, y un emergente interés popular por articular medios alternativos e independientes como contrapoder a los medios de comunicación convencionales y a sus agendas, y contra el oportunismo de los poderes fácticos que convierten su lucha contra el individuo plenamente libre y soberano, emancipado en el ciberespacio, en una lucha contra el terrorismo (Goldstein, 2009: 596).

Frisando el cambio de siglo, Goldstein identificó un cambio comunicacional que amplió las posibilidades del activismo en el ciberespacio:

> A medida que la década llegaba a su fin, nos dimos cuenta de un cambio en la manera en que la gente estaba empezando a hacer frente a estas y otras cuestiones. Cada vez más y más personas se estaban saltando los canales tradicionales de comunicación y difundían sus mensajes simplemente según sus propias condiciones. Blogs, sitios web, audio, vídeo, el poder de la Red se estaba finalmente traduciendo en el sentido de empoderamiento para aquellas personas que no tenían voz en la corriente principal. La gente estaba hablando y más personas estaban escuchando. El movimiento de medios independientes apareció en Internet cuando el mundo se acercó a un nuevo milenio (Goldstein, 2009: 550).

La tensión entre el viejo mundo y el nuevo mundo se agudizó aún más cuando los atentados del 11 de septiembre de 2001 en Estados Unidos dieron lugar a un nuevo orden mundial en el que, según el tecnológo Richard Thieme, "la libertad para moverse sin ser observado", esto es, "la privacidad", se convirtió en "un privilegio exclusivo de los ricos" (Knappenberger, 2012). Si la caída del Muro de Berlín y del Telón de Acero, y la desarticulación de la Unión Soviética produjeron en la década de 1990 cambios en la estrategia geopolítica mundial y una expansión del dominio estadounidense y del capitalismo, mediante la fuerza bruta militar y económica, los atentados del 11 de septiembre de 2001 dieron paso a otras nuevas estrategias expansionistas basadas en la conbinación de nuevos métodos de guerra militar inteligente y la aplicación como nunca antes se había visto del poder blando que los expertos de RAND habían desarrollado conceptualmente, con la seguridad nacional como excusa para el control de la información y datos, y la vigilancia masiva de la población, de organizaciones civiles y de otros gobiernos.

Los atentados del 11 de septiembre de 2001 marcaron un antes y un después para la seguridad y el orden mundial, la privacidad del individuo y las libertades civiles. La seguridad nacional fue la excusa para socavar los derechos que los hackers y libertarios del ciberespacio consideran fundamentales. El Estado-nación emprendió nuevas acciones para intervenir los sistemas de encriptación y cualquier otro que garantice el anonimato en las comunicaciones, otorgándose nuevos y amplios poderes para realizar escuchas telefónicas y monitorizar el tráfico de Internet, con un "abrumador apoyo del público aterrorizado" (Goldstein, 2009: 626). Además, "los acontecimientos del 11 de septiembre pusieron un signo de interrogación sobre el

movimiento antiglobalización", sitiado por un régimen de terror que terminó por redefinir "la disidencia como terrorismo", enfrentando a los activistas y hacktivistas a una represión legal y violenta que terminó por estrechar dramáticamente el espacio de protesta (Jordan y Taylor, 2004: 65).

En los albores del siglo XXI confluyeron varios factores que permitieron la instauración de un nuevo modelo de vigilancia global y ubicua: el uso masivo de la telefonía móvil inteligente, el uso masivo de Internet, la tecnología inalámbrica, la aparición de los medios sociales en línea y la irrupción del terrorismo global como la gran amenaza para la seguridad de los Estados-nación. Paradójicamente, después de que los regímenes comunistas dominados por la extinta Unión Soviética desaparecieron y sus nuevos regímenes se integraron en el capitalismo y se alinearon con Estados Unidos, un nuevo sistema de vigilancia *orwelliano* se ha ido construyendo en Occidente; un sistema de espionaje y control como nunca antes se había imaginado, sustentado en las telecomunicaciones. La infraestrutura de las redes de comunicación electrónicas se convirtió en una arquitectura de control para una nueva era de vigilancia.

El estado de paranoia colectivo tras el 11-S también contribuyó aún más a la valoración social negativa de hackers y hacktivistas, que pasaron de ser considerados delincuentes a ser identificados como ciberterroristas. Así lo constata Vegh (2003) en su análisis cuantitativo y cualitativo de artículos publicados en cinco periódicos estadounidenses —*The New York Times*, *The Wall Street Journal*, *The Washington Post*, *San Jose Morning News* y *USA Today*— en los que aparecen menciones a la palabra *hack*, o cualquiera de sus variantes, antes y después de los atentados. Los resultados de Vegh muestran que la cobertura mediática del *hacking* es generalmente negativa, pero lo fue aún más en los meses posteriores al 11-S. En concreto, identifica una tendencia generalizada a usar el modo condicional, aunque eclipsado por el uso de un lenguaje fuertemente negativo y sensacionalista que incurre en grandes vaguedades sobre los lugares, el momento y la naturaleza de presuntos ataques hackers y sus artífices, lo cual contrasta con la precisión en la definición de objetivos reales o potenciales de estos ataques. Aunque en los meses inmediatamente posteriores al 11-S se constata una disminución de la incidencia de la actividad hacker y hacktivista, su valoración es más negativa que en los meses previos a los atentados. Hackers y

hacktivistas dejaron de ser considerados delincuentes informáticos para ser, cada vez más, identificados en los medios como ciberterroristas, en un clima de temor globar a un terrorismo también global.

El terrorismo se convirtió en la coartada perfecta para controlar las redes de comunicación globales y damnificar si cabe aún más la reputación social de los libertarios del ciberespacio. Por ejemplo, la red de comunicación Tor, que garantiza el anonimato y la privacidad, y protege a sus usuarios de la censura y el control, dando entrada al usuario a lo que se ha dado a conocer como la web profunda, ha sido objetivo de ataques de la National Security Agency de Estados Unidos, como revelan los documentos secretos filtrados por Edward Snowden (Ball, Schneier y Greenwald, 2013).

Los intentos por controlar redes y sistemas de comunicación que garantizan la privacidad y el anonimato se fundamentan en la amenaza de los llamados Cuatro Jinetes del Apocalipsis de la Red: el blanqueo de dinero, el tráfico de drogas, la pornografía infantil y el terrorismo. La retórica ciberapocalíptica ha intentado convencer a la opinión pública de que la criptografía libre aplicada a la navegación web y a las comunicaciones digitales sirve no sólo para proteger a disidentes en países totalitarios, sino también, y fundamentalmente, como refugio de criminales que amenazan la seguridad de las naciones y de los ciudadanos. Los libertarios del ciberespacio argumentan, sin embargo, que estas tecnologías seguras para sus usuarios sirven para proteger a los individuos de los sistemas de vigilancia estatales y globales (Assange *et al.*, 2012: 43, 70, 72) y para esquivar el control que el mercado ejerce sobre los usuarios monitorizados.

La opinión de la comunidad hacker, y especialmente entre los *cypherpunks*, sobre esta delicada y controvertida cuestión la sintetiza de manera clara Jacob Appelbaum, periodista independiente, investigador en seguridad informática, fundador del *hackerspace* Noisebridge en San Francisco, hacker del Chaos Computer Club y miembro destacado del Proyecto Tor:

> […] la respuesta no es destruir el medio, o controlar policialmente ese medio. Se trata de encontrar pruebas para perseguir los delitos que el medio ha documentado. La solución no consiste en debilitar el medio, no pasa por lisiar a la sociedad por completo por un asunto particular (Assange *et al.*, 2012: 135).

Por lo tanto, el uso de tecnología criptográfica para preservar la privacidad no tiene por qué limitar o impedir aspiraciones para acabar con el crimen en el ciberespacio, pero sí "impide que cualquier ataque a través de la fuerza coercitiva pueda funcionar" (Assange *et al.*, 2012: 100).

La importancia de la privacidad como derecho fundamental es tal para los hackers que incluso la propia comunidad penaliza la revelación de contraseñas, porque ni es necesaria ni provechosa para comprender mejor la computación, ni es una acción sofisticada ni útil para la causa de la libertad. Sin embargo, la percepción social del hacker informático hace difícil hacer comprender a los *otros* que el *hacking* es una actividad inofensiva, ya que su imagen delictiva proyectada en la opinión pública viola la percepción que ésta tiene del derecho a la privacidad (Goldstein 2009: 504). Cuando la autoridad identifica al hacker como amenaza para la seguridad pública y nacional, expande la idea de que cualquier ordenador puede ser tomado por un hacker para violar la privacidad de cualquier ciudadano y/o robar información, o para poner en peligro a todo un país. Esta percepción adulterada del *hacking* generada por la autoridad y predicada en los medios de comunicación de masas se convierte en creencia social que cristaliza en fe; fe en la autoridad y en las corporaciones empresariales que almacenan enormes cantidades de datos personales. Hay una creencia popular de que los hackers son los violadores de la privacidad y una fe en quienes realmente gestionan nuestros datos personales, trafican con ellos y violan nuestra privacidad.

Además, el ambiente de sospecha y el temor generalizado al terrorismo global y a cualquier forma de crimen organizado en la Red es tal, que parece justifcarse cualquier método de control, vigilancia y censura, afectando directamente a derechos como la libre expresión, el libre flujo de información, la libertad de movimiento y la privacidad, y a aspiraciones como la transparencia política. "En un régimen de sospechas y temeroso […] los libros, las ideas, la habilidad técnica, todo esto podría ser considerado una amenaza" (Goldstein, 2009: 534). Esa amenaza, hoy, se llama WikiLeaks. Pero antes de abordar este fenómeno que cabalga entre el periodismo, el *hacking*, el activismo y la política institucional, debemos abordar el nuevo contexto informacional que se ha configurado en la intersección en la Red de los viejos modelos de la comunicación de masas y los nuevos modelos de comunicación social que,

principalmente con la popularización de las redes sociales en línea, están reordenando las relaciones entre el Estado-nación y las empresas, por un lado, y los ciudadanos, por otro, mediadas por el uso masivo de tecnologías digitales de la comunicación y la información.

Cuando se descubrió que la información era un negocio, la verdad dejó de ser importante.

—Ryszard Kapuściński.

III. HIPERMERCADOS DE LA INFORMACIÓN EN LA ERA DE LA TRANSREALIDAD

III.1. INTRODUCCIÓN

Hasta ahora hemos visto cómo los hackers han jugado un papel esencial en la transición de la sociedad industrial a la sociedad informacional. El adagio "la información quiere ser libre", que ha guiado a los hackers en su devenir histórico, parece ahora empezar a encontrar, por fin, acomodo en la sociedad, aunque con efectos paradójicos. Las tensiones entre el plagio posmoderno del viejo modelo industrial privativo que quiere permanecer y un nuevo modelo postindustrial abierto que quiere expandirse parecen haberse agudizado aún más en todas las dimensiones que configuran nuestro modelo de vida: la educación, el trabajo, los medios de comunicación, la política, el consumo de bienes y servicios, y las relaciones sociales. Hacia dónde nos dirigimos es aún una incógnita que sólo será resuelta cuando se solucionen estas tensiones a favor del plagio o de la originalidad.

En esa intersección entre lo que ha sido y lo que está empezando a ser, surge WikiLeaks como galvanizador de nuevos valores éticos para los tiempos virales. Por ello, y para acabar de completar este recorrido que hemos emprendido para comprender las esencias de WikiLeaks como fenómeno que surge de las emergencias informacionales, consideramos oportuno ofrecer una panorámica de los nuevos mecanismos de interacción y participación entre medios de información y ciudadanos en la sociedad red que nos permita explicar la razón de ser de WikiLeaks en el nuevo ecosistema comunicacional y que, además, nos sirva para justificar la radical importancia que tiene medir el impacto mediático de un fenómeno como éste para su comprensión.

En este capítulo veremos cómo en la era de la transrealidad, en la que los límites espacio-temporales se diluyen, surgen nuevos autores y voces que contribuyen a estirar la larga cola que, paradójicamente, nutre a la cabeza del mercado y contribuye a mantener estructuras de dominio y poder tradicionales. Analizaremos también cómo el deseado *feedback*, lejos de cumplir una función emancipadora, es una herramienta fundamental para controlar a los usuarios, que han entregado su privacidad a grandes corporaciones a cambio de visibilidad y atención. Y se explicará la estrategia de desprofesionalización del periodismo y la mutación de los medios de información en meros agregadores como vía para la fagocitación, control y explotación económica de la larga cola, además de describir cómo intermedian los nuevos *influencers* en las nuevas relaciones entre medios y ciudadanos.

III.2. TRANSREALIDAD

Vivimos una era en la que estamos superando lo *pluri*, lo *multi* y lo *inter*, transgrediendo los límites físicos y cognitivos espacio-temporales —las dimensiones fundamentales de la vida humana—, para conectarnos *a través de* y *al otro lado*. Es la era de la transrealidad, en la que nuestra percepción del espacio y del tiempo se ha visto alterada y lo virtual y lo real se enredan en el hiperespacio.

> Dimensiones básicas de la vida como el tiempo y el espacio se deconstruyen, y la interacción tiene lugar en un mundo globalizado en el que todos los procesos convergen en un solo proceso, en tiempo real, en todo el planeta (Pacheco, 2011: 37).

El nuevo paradigma comunicacional se presta a ello:

> El tiempo se borra en el nuevo sistema de comunicación, cuando pasado, presente y futuro pueden reprogramarse para interactuar mutuamente en el mismo mensaje. El espacio de los flujos y el tiempo atemporal son los cimientos materiales de una nueva cultura, que trasciende e incluye la diversidad de los sistemas de representación transmitidos por la historia: la cultura de la virtualidad real, donde el hacer creer acaba creando el hacer (Castells, 2001: 452).

La nueva transrealidad es configurada por lo transpolítico, lo transcultural, lo transhistórico, lo transmoderno, lo transnacional, lo translocal, lo transglobal, lo transfronterizo, lo transmedia, lo transexual, lo transdisciplinario, lo transversal. Realidades *trans* que ya anticipó Baudrillard:

> Cada categoría es llevada a su mayor grado de generalización perdiendo con ello cualquier especificidad y reabsorbiéndose en todas las demás. Cuando todo es político ya nada es político, y la palabra carece de sentido. Cuando todo es sexual, ya nada es sexual y el sexo pierde cualquier determinación. Cuando todo es estético ya nada es bello ni feo, y el mismo arte desaparece. Este paradójico estado de cosas, que es tanto la realización total de una idea —la perfección del movimiento moderno— como su denegación —su liquidación por su mismo exceso, por su extensión más allá de sus propios límites—, puede ser reconquistado en una misma figura: transpolítica, transexual, transestética" (Baudrillard, 1991: 16).

Lo *trans* es la indiferenciación entre lo real y lo virtual, entre el espacio físico y el espacio cíber, entre lo real y lo ficticio, entre lo cierto y lo falso, entre el original y la copia, entre lo palpable y lo etéreo, entre lo lejano y lo cercano, entre lo distintivo y lo genérico, entre lo clásico y lo contemporáneo, entre el presente *revival* y el presente prospectivo, entre el entretenimiento y la información, entre lo global y lo local que se

funden en la promiscuidad de lo *glocal*. Realidad de realidades micros y macros, híbrida, mutante, líquida (Bauman, 2003), hipermoderna y acelerada (Lipovetsky, 2006), e hiperespacial. La sociedad civil se ha transnacionalizado. Y lo transnacional es translocal y transglobal. *Transglocalización* en tiempos hipermodernos de desterritorialización:

> Para existir un mayor control del ciberespacio, los Estados tienen que perder soberanía: deben converger esfuerzos y compartir el poder. A lo largo de la historia, el control de la información ha sido la esencia del poder de los Estados. En esta coyuntura, por un lado, estamos positivamente desterritorializados, es decir, emergen a través de la red nuevos movimientos transnacionales sociales, políticos y culturales, los cuales cada vez más se constituyen como poder de oposición a lo instituido y permiten que las voces que antes eran ignoradas ahora sean escuchadas (Pacheco, 2011: 37).

Para comprender aún mejor esta transrealidad debemos entender que nuestra percepción del mundo es ahora transmediática, una idea que "propone una versión ampliada del concepto aristotélico de *sensus comunis* (no traducible pero relacionado con el sentido común), entendido como una sensación en el individuo coordinada hacia una comunidad social extendida ahora globalmente" (Suárez Puerta, 2009: 188). El todo, la historia, se nos cuenta a través de múltipIes plataformas mediáticas, y cada nuevo texto hace una contribución específica y valiosa a la totalidad (Jenkins, 2008: 101).

Vivimos en una realidad *trans* en la que todo fluye atravesando y transgrediendo el espacio y el tiempo. Una realidad como relato, en sentido *barthesiano*:

> En sus casi infinitas formas, el relato está presente en todas las épocas, en todos los lugares, en todas las sociedades; el relato comienza con la historia misma de la humanidad; no hay y nunca ha habido en ningún lugar un pueblo sin relato. Todas las clases, todos los grupos humanos tienen sus relatos, y muy a menudo esos relatos los disfrutan en común hombres de culturas diferentes, incluso opuestas: el relato se burla de la buena y de la mala literatura: internacional, transhistórico, transcultural, el relato está ahí como la vida (Barthes, 1966: 1).

Si aceptamos que la nueva ideología del capitalismo propone un nuevo paradigma organizativo, "la empresa sin frontera, descentralizada y nómada" (Salmon, 2008: 111), y que la vida de las sociedades neoliberales se presenta como una inmensa acumulación de historias (Salmon, 2011: 19), vemos entonces que el nuevo paradigma

comunicacional apuntala la lógica neoliberal mediante la acumulación de múltiples relatos que fluyen *a través de* y *al otro lado de* nodos conectados en red.

Múltiples voces y versiones, en múltiples medios, soportes, formatos, plataformas y géneros, convergen en un espacio global y contribuyen a conformar esta realidad *trans*. Una realidad en la que se alteran la noción de distancia y el vínculo lineal entre pasado, presente y futuro. Realidad que se configura en un hiperespacio atemporal, en el que se conectan el espacio cíber y el espacio físico, y donde se desarrollan y fluyen los múltiples relatos, sin principio ni fin; no sólo los grandes relatos, sino también los relatos personales, los relatos de lo privado, volcados ahora en el dominio público en un éxtasis comunicacional. Es precisamente de la permanente construcción pública del relato personal en una realidad líquida y global de donde emergen los moldes de identidad, los personajes *virtuales* en los que nos refugiamos para vivir hiperconectados; nuestros *yoes* líquidos.

La realidad desterritorializada, ubicua, multicrónica, transnacional, trasnmediática y *transglocal* plantea enormes retos en un mundo en el que se globalizan mercancías, servicios, conflictos, crisis, políticas neoliberales, ideas y hábitos de consumo y estilos de vida, a la vez que se fortifican las fronteras físicas contra el libre movimiento de individuos y se intenta hacer lo propio levantando vallas virtuales en el ciberespacio.

III.3. MÚLTIPLES MEDIOS, MÚLTIPLES RELATOS

La multiplicidad de relatos que convergen en el hiperespacio ha sido favorecida por la universalización del acceso a Internet, el abaratamiento de la tecnología digital y la democratización de herramientas de producción y distribución en línea. Un proceso que ha permitido también la irrupción de nuevos cibermedios que permiten la aparición de nuevos autores, voces e intermediarios en el hiperespacio, con relatos inéditos que, o bien vigorizan el discurso principal, o bien difieren del relato oficial dominante e incluso lo contradicen. Los llamados medios alternativos parecen cuestionar el mandato de los medios de comunicación tradicionales, su función de intermediarios y la *exclusividad* y dominio de sus relatos. Es así como la historia ya no se explica con una versión oficial lineal, sino que se (poli)construye mediante la acumulación, diseminación y confrontación de múltiples relatos accesibles en cualquier momento y en cualquier lugar.

Desde blogs, hasta periódicos digitales independientes, pasando por los medios de comunicación unipersonales que los *influencers* —los nuevos líderes de opinión— mantienen en Twitter o Facebook, todos ellos alteran el *statu quo* mediático de la sociedad de masas. La aparición de una larga cola de medios y relatos modifica nuestro paisaje y nuestra aproximación a la realidad. Esa larga cola es la que ha aparecido para ofrecernos aquello que nos falta por acción u omisión de los medios de información dominantes, que han diseñado tradicionalmente la agenda de temas para nuestra socialización. Así, "el poder de los medios populares reside en su capacidad de diversificar", mientras que "el poder de los medios masivos reside en su capacidad de amplificar" (Jenkins, 2008: 255).

La Teoría de la Larga Cola, formulada por Chris Anderson en octubre de 2004, en un artículo en la revista *Wired*, señala que hemos pasado de una economía basada en la escasez a otra basada en la abundancia, del mercado de masas al mercado de nichos: nuestra cultura y economía están migrando del tradicional enfoque en el alto consumo de unos pocos productos y servicios populares (la cabeza del mercado), hacia un consumo de productos y servicios más variados, aunque menor (la cola del mercado). Esta tendencia favorece la fragmentación de la audiencia hasta desarrollar una hiperfragmentación de la misma. Es el *universo* hecho trizas. Las pequeñas historias de muchos emisores se acumulan en la larga cola. Pasamos así de los medios

de masas a la masa de los medios (Ramonet, 2011), del absolutismo de los medios de masas, a la cultura participativa de los medios sociales (Jenkins, 2008), y de la exigüidad, a la sobreabundancia de relatos y versiones.

Ahora bien, este proceso de democratización en la producción y distribución de contenidos está intervenido por la paradoja del control en Internet (Karp, 2006): la libertad de expresión y de creación digital, gracias a las nuevas herramientas tecnológicas, aumenta los creadores y las obras, pero el control de la comercialización y del rendimiento económico se concentra cada vez más en menos manos a través de una recentralización. Es decir, mientras en la larga cola de Internet cientos de millones de usuarios nutren la red de contenidos a cambio del uso *gratuito* de herramientas para producir y distribuir contenidos, y de atención y posicionamiento, la cabeza de la Red acapara los recursos y beneficios económicos y se fortalece, de manera que los resortes de Internet van siendo concentrados por el oligopolio de Google, Facebook, Amazon, Apple, Microsoft, etc. "MySpace, Facebook y muchos otros negocios se han dado cuenta de que se pueden regalar las herramientas de producción y mantener la propiedad sobre los productos resultantes" (Carr, 2006). Así, no sólo nos ofrecen las ventanas de acceso a la totalidad de la realidad, sino que además controlan y rentabilizan los contenidos que producimos y compartimos en sus repositorios a cambio de los quince minutos de fama que Andy Warhol nos prometió. Es el capitalismo tecnológico.

III.4. MEDIOS TRADICIONALES *VS* MEDIOS SOCIALES: EL MODELO 'HUFFINGTON POST' DE PERIODISMO LÍQUIDO PARA LA SOCIEDAD NEOLIBERAL

En el escenario que hemos descrito hasta ahora convergen los medios tradicionales de masas y los denominados medios sociales *online*, produciéndose en su encuentro la tensión entre el viejo modelo periodístico y el nuevo modelo de producción y distribución de información. *The Huffington Post* es el paradigma de la comercialización *exitosa* de esa tensión en el nuevo ecosistema (Quian, 2012).

El modelo *HuffPost* se sostiene en tres puntos clave: 1) crear una estructura empresarial flexible y líquida, de costes económicos reducidos al máximo e integrada en un conglomerado mediático transnacional, AOL; 2) integrar en la estructura periodística un repositorio global de blogs, cuyos autores reciben como única remuneración visibilidad y atención, y 3) desarrollar una estrategia SEO (*Search Engine Optimization*) que supedita los contenidos a los algoritmos de Google y demás buscadores para estar en lo más alto del ránking de visibilidad. Es así como se produce lo que consideramos la paradoja de la larga cola en una nueva lógica económica informacional: el medio en la cabeza del mercado es nutrido por la larga cola de blogs; o dicho de otra forma: la larga cola de nichos especializados mantiene al viejo modelo de masas en la cima de la curva de la demanda. En esta nueva lógica, el dador espera a cambio una gratificación en forma de estímulo, el de una droga aún más dura que el dinero en la era de las masas creadoras: visibilidad y atención mediante e su exposición en un medio global ciberespacial.

La economía de la atención es la que facilita un mercado donde los individuos aceptan recibir servicios a cambio de su atención (Iskold, 2007) o los prestan para recibir como remuneración la atención de otros. Hoy, se está haciendo popular en nuestra sociedad de un nuevo bienestar simbólico clasificar los ingresos de la atención por encima de los ingresos de dinero. Es un paso más allá en la ética protestante, en la que la fama se convierte en el eje motivador de la actividad productiva del individuo en las sociedades informacionales, mientras unos pocos rentabilizan el trabajo de unos muchos.

> La atención de los otros es la más irresistible de las drogas. Por eso la gloria sobrepasa al poder y por eso la riqueza es ensombrecida por la preeminencia. El indiscutible común denominador de las elites es la preeminencia, que no es sino el

> estado de lograr la mayor atención. Por eso llegar a ser popular y atraer la atención es más importante que la riqueza económica (Franck, 1999).

Tenemos así un modelo de bajo coste y alto rendimiento económico que se aplica a un medio global como el *Huffington Post* y que se basa, principalmente, en la dación de contenidos de una red de colaboradores a cambio de atención para éstos y en la tiranía algorítmica de Google. Es el modelo de la inmensa acumulación de relatos de las sociedades neoliberales, centrado en el acto de comunicar-informar como entretenimiento, como pasatiempo, como mero espectáculo. Así lo reconoce la propia Arianna Huffington:

> Somos una plataforma en la que ofrecemos distribución a miles de personas que superen un listón de calidad. No se la dejamos a cualquiera. Pero si tienes ese nivel, seas o no conocido, puedes estar en la plataforma de *The Huffington Post.* Así puedes llegar a una gran audiencia, en nuestro caso enorme gracias a la unión con AOL. Los comentarios son moderados previamente, con lo que entras en una conversación de calidad. Si quieren o no bloguear es su opción. Nadie va a llamarles para decirles que blogueen, no se crean expectativas, no hay plazos. Hay mucha gente que no lo entiende porque es un nuevo modelo, no comprenden por qué hay personas que bloguean gratis, o por qué actualizan la Wikipedia sin cobrar, o su muro de Facebook. Comunicar es el nuevo entretenimiento de la gente. Es una nueva fuente de autorrealización. Nadie se pregunta por qué hay gente que se pasa horas viendo mala televisión gratis. Todavía no nos hemos ajustado a la nueva realidad de cómo la gente quiere vivir sus vidas. En cuanto a la agregación, aunque tuviera un presupuesto ilimitado seguiría haciéndolo. Es un servicio a mis lectores. Si mi compromiso es mostrar lo mejor, algunas historias las produciremos nosotros y otras las escogeremos, las filtraremos de otros sitios (Echevarría, 2011).

Este modelo ha *infectado* a *Le Monde* en Francia, a *El País* en España y a *L'Espresso* en Italia, que en el año 2012 concretaron un acuerdo de colaboración con la nueva *gurú* de las empresas informativas, Arianna Huffington, para clonar su *exitoso* modelo de negocio. Éxito que excluye la variable cualitativa y que se mide casi exclusivamente en cantidades. Es el triunfo del modelo informativo neoliberal, "basado en la abundancia de contenido de bajo coste, con la opinión, la suma de contenido ajeno y la optimización en buscadores (SEO) para conseguir el máximo de tráfico" (Varela, 2011).

The Huffington Post es el medio que mejor ha entrecruzado la paradoja del control, la economía de la atención y la Teoría de la Larga Cola, en la que ya se nos advertía de que es sólo mediante la agregación de contribuciones a gran escala —en

una escala web— como se convierte en lucrativo un negocio (Carr, 2006). Es, en definitiva, el modelo de la banalización del periodismo, la expansión de áreas de "noticias blandas" (Gans, 2003), la producción de información como *hobby*, su consumo como entretenimiento, la anécdota sobrevalorada y el clímax de la superioridad del *opinionsharing* sobre el *newsharing* (la opinión prima, tanto, que parece el único motor que sostiene Internet; he ahí la clave: todos quieren opinar, todos quieren influir, todos quieren gobernar). Y lo banal narcotiza.

Paul Lazarsfeld y Robert Merton nos introdujeron en 1948 en las consecuencias que producen los medios cuando saturan a las audiencias con contenidos intrascendentes, alejándolos de las problemáticas sociales de importancia y convirtiéndolos en meros espectadores de un mundo ocioso, superficial y trivial. Ahora se produce un *aggiornamento* de la disfunción narcotizante hacia la que se nos empuja en pleno auge de un nuevo modelo de sobreabundancia de intereses personales agregados en espacios de acceso masivo, donde son mercantilizados.

Parece, pues, que los medios de información de masas podrían dejar de ser productores de información, o al menos reducir esta función, para convertirse en agregadores de contenidos de medios personales especializados, con nuevas temáticas y nuevas formas de pensar, producir y distribuir la información. Es, al menos hasta ahora, el modelo de *éxito* económico en Internet, donde ninguna de las grandes corporaciones que dominan el ciberespacio es creadora de contenidos, sino que se nutren y se mantienen en la cima de la curva de demanda masiva gracias a la larga cola (Google, Amazon, Facebook, Twitter… y ahora también las empresas informativas). Recordemos: "Una característica económica fundamental de la Web 2.0 es la distribución de la producción en manos de muchos y la concentración de los beneficios económicos en manos de unos pocos" (Carr, 2006).

The Huffington Post es el mensaje (o el masaje) en sentido *mcluhiano*. No importan tanto los contenidos como su suma y jerarquización; no importan tanto las palabras e imágenes como los efectos que la nueva estructura de producción, distribución y consumo causa en los usuarios; no importan tanto los múltiples relatos que se suceden a un ritmo endiablado como el medio que los vehicula y el uso que los prosumidores hacen de las herramientas que les ofrece el medio. El medio es el mensaje. Y si el medio es el mensaje, nosotros, internautas y prosumidores, también

somos el medio. Vivimos por la economía de la atención, en el altar de la egolatría en el que hemos convertido Internet. Cuanto más arriba nos vemos en el ránking de Google, más vivos nos sentimos. Estamos presentes, estamos vivos. Me ven (los motores de Google), *ergo* existo.

Para terminar de describir la situación es necesario atender a algunas paradojas que envuelven a los medios periodísticos tradicionales, hasta ahora dominantes, en su intento por resolver su futuro incierto. Aunque siguen creciendo tanto el flujo de información *online* como la cuota de los diarios digitales, la facturación sigue siendo modesta para mantener mastodónticas y rígidas estructuras —más propias de la sociedad industrial—, a la vez que desciende la difusión del papel y la publicidad en este soporte. La rentabilidad de los medios periodísticos tradicionales ahora digitalizados es aún un futurible. Para los que resisten, buena parte de su negocio sigue estando, paradójicamente, en un soporte tan decadente para los nativos digitales como el papel. Esto nos lleva a otra paradoja: los medios híbridos con ediciones en papel y digitales diseñan planes cada vez más sofisticados para desarrollar sus estrategias en la Red, a la vez que invierten ingentes esfuerzos técnicos y humanos y enormes cantidades de dinero en proteger sus ediciones en papel. Un buen ejemplo lo encontramos en *La Voz de Galicia*, periódico que aunque ha dado gran impulso a su edición digital y a su estrategia en redes sociales, siendo uno de los diarios en España mejor posicionados en Internet, invirtió en el año 2010 una astronómica cantidad de dinero para renovar su rotativa: 25 millones de euros dedicados a modernizar un producto en claro declive. Inversiones generosas de dinero y de esfuerzos, de un altísimo riesgo en un entorno cambiante y en medio de una crisis económica y de identidad periodística que ponen contra las cuerdas a los diarios impresos y a las ediciones digitales que se mantienen de la rentabilidad que aún conserva el papel, principalmente por las ayudas públicas que todavía recibe.

Vamos con otra paradoja: las empresas periodísticas no han sido ajenas a la profunda crisis económica global que nos ha deprimido desde finales del año 2007, a la que hay que sumar la crisis de identidad de la profesión y la crisis de credibilidad que padece por culpa de un modelo de periodismo mercantilizado, politizado, subvencionado y precarizado. La idea de que las nuevas tecnologías han incidido en la crisis de los medios es una visión distorsionada de la realidad. Las grandes empresas

informativas cuentan con algunos de los mejores especialistas en la materia liderando sus equipos digitales, contratan a los mejores consultores y hacen grandes inversiones en tecnología para ofrecer los servicios más avanzados a sus usuarios y para estar en la vanguardia en diseño y usabilidad web. Y, sin embargo, su imagen y reputación se debilitan entre los ciudadanos, como han atestiguado en España el informe *Esporas de helechos y elefantes*, publicado por la Fundación Compromiso Empresarial (Morales Steger, Irisarri Núñez y Martín Cavanna, 2011), y en Estados Unidos, el estudio *Views of the News Media: 1985-2011*, del Pew Research Center for the People & the Press (2011).

El problema real es que cada vez más en la calle y en las redes sociales los ciudadanos hablan de crisis del modelo de periodismo, de sus pobres contenidos, de su función social, de su falta de transparencia y de ética, mientras los medios y sus profesionales, aparentemente ajenos a su crisis de contenidos y al clamor popular, están narcotizados por el debate sobre los modelos de negocio y los efectos de las nuevas tecnologías en el propio negocio. La crítica social se ha acrecentado con la irrupción de WikiLeaks como contrapoder al supuesto contrapoder del periodismo de los medios convencionales. Hoy, el problema real del periodismo no es el modelo de negocio, pero el principal problema del *negocio* periodístico sí es el modelo de periodismo que se está haciendo. Y no hay mejor modelo de negocio que el buen ejercicio periodístico.

Precisamente, la crisis económica y de reputación del periodismo introduce otra paradoja: el intento de *revitalizar* la profesión y el sector reduciendo la oferta de medios de información y, por lo tanto, el número de periodistas. El escenario ideado por algunos editores es el siguiente: pocos medios, menos competencia, menos periodistas y más colaborares gratis. En España, Bieito Rubido, director del diario *ABC*, hizo manifiesto en noviembre de 2011, en un encuentro en el Foro de la Nueva Comunicación, su deseo de restringir la oferta informativa mediante un oligopolio mediático: “Sobran la mitad de los periódicos, de las emisoras de radio, de las cadenas de televisión y, aunque sea muy duro decirlo, sobramos la mitad de los periodistas” (El Mundo, 2011). Es decir, Rubido quiere cargarse la larga cola y estrechar aún más la cabeza del mercado mediático para devolvernos a la economía de la escasez, a una oferta de masas aún más comprimida y menos plural.

Rubido siente amenazada la supremacía y *exclusividad* que hasta hace bien poco conservaron los viejos medios de la sociedad industrial, que ahora observan con pavor la irrupción de nuevos medios alternativos gracias a Internet, al abaratamiento y democratización de la tecnología digital, y a los reducidos costes de producción y distribución de la información. Hoy, medios locales, regionales, nacionales y globales, viejos y nuevos, industriales y digitales, incluso medios unipersonales, compiten en aparente igualdad de condiciones en un mismo espacio por el que transitan cientos de millones de nómadas de la información y del entretenimiento.

El modelo *HuffPost* y el de Rubido son dos caras de una misma moneda: uno pretende fagocitar la larga cola de blogs y el otro quiere cerrar medios y facultades de periodismo para estrechar la oferta con el fin, ambos, de centralizar el *negocio* de la información en pocas manos. Es la jugada *perfecta* de algunos editores y directores de corporaciones mediáticas: construir negocios informativos en los que ellos (unos pocos) se benefician a costa de unos periodistas precarizados y reducidos al máximo posible, y de la producción de una masa de dadores que se sienten suficientemente retribuidos y gratificados con la visibilidad y atención que les proporcionan los medios (nuevo paradigma de la Teoría de los Usos y Gratificaciones). La trampa está hecha.

Otra paradoja que se produce es que la deseada inmediatez y el tiempo real ininterrumpido que ofrecen las redes sociales en línea, bien gestionados, benefician el ejercicio del periodismo como nunca antes; sin embargo, la inmediatez también puede tener efectos perversos si no es bien administrada y digerida. La verificación de datos y hechos es uno de los grandes retos a los que se enfrenta el periodismo en la era de la sociedad red, al que no debe renunciar si no quiere sucumbir al ruido, al rumor y a las falsedades que circulan con descaro por Internet. Cada vez es más imperiosa la intervención de los verificadores de datos (*fact-checkers*), figuras que adquieren un papel determinante para distinguir la información veraz de los rumores, de las manipulaciones, de las mentiras, de lo inexacto, en un nuevo ecosistema *infosaturado*, donde sobreabundan los contenidos, donde nos vemos desbordados por avalanchas de información pero también de desinformación, y donde las emociones, pasiones y obsesiones personales son elevadas al estatus de verdades universales distribuidas por redes sociales en línea como Twitter. En *Twitter as a Vector for Disinformation*, estudio publicado en 2010 en la School of Computer & Security Science de la Edith

Cowan University (Australia), se nos advierte de que igual que todas las redes sociales, Twitter es vulnerable a ataques de desinformación, aunque Twitter es especialmente susceptible debido al formato informal de los mensajes y la estructura asimétrica de la relación entre los nodos de la red.

Nos manejamos, por lo tanto, en nuevos espacios donde todo fluye y se distribuye sin control aparente a velocidades vertiginosas, en una suerte de perfecto caos comunicativo en el que adquiere especial importancia el verificador de datos y hechos: ¿la foto está trucada?, ¿el vídeo es un montaje?, ¿es cierto lo que se dice en Twitter?, ¿qué credibilidad tiene la fuente?, ¿de dónde proceden esos datos? Pero este trabajo de verificación implica un consumo de tiempo del que *no* dispone el medio que se somete a la dictadura de la inmediatez que impera hoy en día.

Mentiras, rumores y hechos y datos no verificados circulan con desvergüenza por blogs y redes sociales. Veamos algunos de los muchos casos que se han hecho populares. Por ejemplo, las falsas fotografías que se publicaron del huracán *Irene* en agosto de 2011 supuestamente golpeando la costa de Carolina del Norte y que se distribuyeron por redes sociales y blogs. Algunas de las imágenes que se compartieron masivamente no eran de *Irene*, sino de fenómenos meteorológicos extremos ocurridos tres semanas antes en Pensacola, Florida (Bilton, 2011).

Ilustración 15: Foto tomada en Pensacola (Florida) que fue distribuida en Internet como el momento de la llegada del huracán *Irene* a Carolina del Norte.

Fuente: *The New York Times*.

Recordemos también la fotografía de un tiburón supuestamente buceando por las calles de Puerto Rico tras el impacto de *Irene*, una fotografía que resultó ser también un *fake*, una imagen trucada que se distribuyó en el popular canal de marcadores sociales Reddit y que se viralizó por redes sociales, blogs y algunos medios de información (Hughes, 2011).

Ilustración 16: Imagen trucada de un tiburón en las inundadas calles de Puerto Rico.

Fuente: Reddit.

O el caso de una ciudadana estadounidense que se autodefine sin ruborizarse "bloguera de investigación", condenada por difamar reiteradamente en Internet a un abogado. Esta mujer, llamada Crystal Cox, acusó al abogado Kevin D. Padrick y a su empresa, la compañía de inversiones Obsidian Finance Group, de ser investigados por cometer presuntamente fraude fiscal, lavado de dinero, robo y soborno. Era una gran mentira, un relato falso de esta bloguera, cuya estrategia era posicionar sus denuncias en los primeros lugares de los motores de búsqueda en Internet, consiguiendo el *éxito* que buscaba, que no era otro que tráfico y notoriedad. Cox tuvo que someterse a la justicia y en diciembre de 2011 fue condenada por difamación a pagar 2,5 millones de dólares en concepto de reparación de daños morales y económicos, pero el daño real, el causado a la reputación de este abogado, fue irreparable (Carr, 2011b). La pregunta es: ¿están todos los autoproclamados periodistas ciudadanos dispuestos a asumir principios éticos, responsabilidades civiles y penales, y las sanciones sociales que puedan derivarse de una comunicación pública que incurra en falsedades, difamaciones, manipulaciones, etc.?

Con demasiada frecuencia vemos cómo se viralizan por blogs, redes sociales y medios de información dominantes y alternativos todo tipo de contenidos falsos. Más que una sociedad de la información y del conocimiento, podríamos estar germinando una sociedad de la credulidad y de la ingenuidad. Y en esto parece tener mucho que ver el sello de veracidad que se le ha puesto a Internet, como si fuese en sí misma la *verdad*. Lo he visto en Internet, luego es verdad.

III.5. CONTROL A TRAVÉS DEL *FEEDBACK*

Para acabar de redondear el negocio de la comercialización de la participación ciudadana, el *feedback*, que pensamos que nos iba a emancipar y a liberar del imperio de las estructuras de poder (Enzensberger, 1970), se convierte en poderosa herramienta para el control de los usuarios por parte de los medios dominantes, ya que el acceso generalizado al *feedback* incrementa dinámicas preexistentes y el poder de mediación lo siguen manteniendo los mismos (Baudrillard, 1981). Es la otra parte de la dación de los ciudadanos: los dadores ofrecen sus contenidos, pero también ceden información personal y su privacidad. En compensación, los usuarios son gratificados con el uso y disfrute de las herramientas de producción y distribución, y con mensajes *personalizados*. Es así como se produce una gratificación mutua: los medios obtienen información personal de sus usuarios para vender a los anunciantes y para diseñar sus estrategias de comunicación y de contenidos, y los usuarios, a cambio, reciben mensajes adaptados a los comportamientos, rutinas y necesidades que comparten con otros segmentos de población (*behavioral targeting*). En este sentido, nada ha cambiado: el público sigue siendo mercancía en manos de los medios de comunicación para que éstos se la vendan a anunciantes y publicistas. Pero lo que sí cambia es tanto la escala como la fiabilidad de la información con la que trafican los medios, que ahora disponen de más datos demográficos y de información más fiable sobre los comportamientos, gustos, tendencias y opiniones de los individuos gracias a toda la información que les servimos navegando por la Red.

Es cierto que el *feedback* siempre ha existido, pero la diferencia es que ahora se produce dentro del medio. Si en los medios tradicionales la obtención de datos requería adoptar una actitud activa por parte de las empresas, ahora éstas reciben toda la información de los usuarios de forma gratuita y constante a través del *feedback* reportado por los internautas en su navegación e interacción. La comunicación interactiva en Internet deja huellas, de manera que el emisor tiene más control sobre la valoración de la información y sobre su difusión y uso. Informarse en un medio *online* es dar *feedback* al medio (volvemos a Baudrillard). Participar en la conversación 2.0 es dejar nuestras *huellas dactilares* y *ADN* digitales en manos de analistas del mercado que, como un Gran Hermano, nos monitorizan constantemente. Estar informado implica, pues, suministrar información a recolectores y traficantes de datos.

Estar informado en la era de la sociedad red obliga a ser visible. Y ser visible implica también ceder información, exponerse en público y ser escrutado y vigilado constantemente, como en el modelo panóptico carcelario ideado en 1791 por Jeremy Bentham y adoptado por Foucault ([1975] 2008), que hoy sirve como metáfora para explicar cómo la continua exposición y visibilidad del individuo en Internet favorece la vigilancia masiva constante, pero no manifiesta, por parte del poder. Los internautas han aceptado e interiorizado mecanismos y rutinas de comportamiento *necesarios* para interactuar en la Red y gozar de visibilidad y atención, a cambio de ser monitorizados. Una lógica que legitima el control *parental*, haciendo de cada ventana, de cada nodo de la Red, una torre de vigilancia desde la que cada individuo observa a los *otros*, convirtiendo, paradójicamente, la naturaleza rizomática de Internet en una estructura de control global en la que todos somos vigilantes y vigilados. Es la hipervigilancia cotidiana y universal en la hipermodernidad descrita por Lipovetsky (2006).

Tal exposición permite al supremo vigilante sofisticar su sistema de control, modelado y prevención de comportamientos sociales aprovechando el desarrollo prodigioso de la ciencia computacional y de sistemas de monitorización, procesamiento y análisis de información y de datos masivos aplicados a las redes de comunicación, como así lo demuestran las revelaciones de Edward Snowden sobre el sistema de vigilancia masiva articulado por la Agencia de Seguridad Nacional de Esados Unidos. En este nuevo estado de vigilancia corporativo-gubernamental a escala global, el Gran Hermano *postorwelliano* sustituye la propaganda por algoritmos, la retórica por matemáticas, la aplicación de la fuerza física por el control de la tecnología, la vigilancia *dura* por la vigilancia *blanda*. El Gran Hermano *postorwelliano* es matemático, estadístico y computacional. Código informático, *big data*, minería de datos masivos y análisis predictivo se usan para suministrar de forma incesante datos e información a gobiernos y corporaciones empresariales y satisfacer así sus hambrientos y cada vez más dilatados *estómagos*.

En definitiva, nunca antes se había cumplido con tanta precisión el axioma de que la información es poder. Si el poder de influencia de un medio de comunicación se mide por su nivel de incrustación en la vida de las personas, Internet lo ha hecho de una manera radical, como ningún otro medio. Y su control por poderes estatales y corporativos lleva a la Red a configurarse en un medio de vigilancia global.

III.6. EXHIBICIONISMO OBSCENO DE IDENTIDADES DE DOMINIO PÚBLICO

Las redes sociales en línea han favorecido la aparición de camaleones sociales que adoptan fragmentos de identidad según convenga (Gergen, 1992). Así, tenemos a nuestro alrededor ciberespacial distintos seres en permanente construcción en los que el pasado no tiene un valor biográfico sólido, sino que se sesga y se reinterpreta para construir una identidad líquida presente y para improvisar la narrativa vital. Para adaptarse a la experiencia multicrónica y ubicua, a la convergencia del espacio físico y del ciberespacio en un hiperespacio, a la realidad *trans*, a la sociedad red y líquida, el individuo adopta las condiciones psicológicas apropiadas, "un yo maleable, un *collage* de fragmentos que no cesa de devenir, siempre abierto a nuevas experiencias" (Sennett, 2000: 140).

Construimos así nuestra identidad virtual de dominio público, en la que se manifiestan las actitudes e ideas subyugadas por los límites físicos, sociales e institucionales de la vida real:

> Nuestra identidad social, la persona que asumimos ser en nuestra interrelación social, es ya una «máscara», ya que implica la represión de los impulsos que no nos resultan admisibles. Sin embargo, es precisamente bajo las condiciones de «tan sólo es un juego» —cuando las reglas que regulan los intercambios en nuestra «vida real» son suspendidas temporalmente— que nos podemos permitir desplegar estas actitudes reprimidas. Pensemos en la notoria figura del impotente y tímido que, mientras participa en un juego interactivo en el ciberespacio, adopta la identidad de un asesino sádico o de un seductor irresistible. Es demasiado simple decir que esta identidad es tan sólo un suplemento imaginario, una huida temporal de la impotencia en su vida real. Más bien la cuestión es que, puesto que él sabe que el juego interactivo en el ciberespacio es «tan sólo un juego», puede «mostrar su verdadero yo» y hacer cosas que nunca haría interactuando en la vida real. Tras la apariencia de una ficción, se articula la verdad sobre uno mismo. El mismo hecho de que perciba mi propia autoimagen virtual como mero juego me permite suspender los obstáculos habituales que evitan que haga efectivo mi «lado oscuro»; en el ciberespacio se da alas a mi *Ello* (Žižek, 2007)[108].

Pero en esta construcción permanente de identidades líquidas (Bauman, 2003) de dominio público hay algo *huellebecquiano*. El nuevo *ser* en construcción es un clon *mejorado* del *yo real* que se conecta al mundo a través de una pantalla, y al que se le ofrece la posibilidad de una *isla*, un nodo más entre los millones de nodos interconectados en red.

[108] Todas las citas tomadas de Žižek son traducciones propias del texto original, en inglés.

El ser hipermoderno en red se socializa, paradójicamente, desde la soledad, desde la experiencia individual, única e intransferible, del acceso al ciberespacio a través de una pantalla unipersonal:

> El típico internauta de hoy, sentado solo frente a la pantalla de un PC, se está convirtiendo cada vez más en una mónada sin una ventana directa a la realidad, encontrando solamente simulacro virtual, y aun así, cada vez más inmersa en la red global, comunicándose simultáneamente con el planeta entero (Žižek, 2007).

Como en la novela *La Posibilidad de una Isla*, de Houellebecq (2005), nuestros clones virtuales se aíslan en cubículos, se comunican con los demás a través de Internet, abandonan progresivamente el contacto físico y el lenguaje no verbal pierde valor comunicativo. La búsqueda del contacto virtual, de la comunicación a distancia, evidencia la soledad del individuo hipermoderno. Es la era de las soledades interactivas y de la obsesión por estar localizables (Wolton, 2000). Nos aislamos en soledad y en compañía, pues es la pantalla de la experiencia unipersonal la que nos conecta con la realidad total: el salón en el que me acomodo, la mujer que me *acompaña*, el televisor y la radio que ambientan, el ruido exterior de la vida en la calle, no son más que elementos parciales, fracciones y fragmentos de la totalidad, como lo son los productos de los medios de comunicación, parciales, sesgados, porciones de una totalidad que por fin tenemos a nuestro alcance y transgrede las limitaciones físicas espacio-temporales que han impedido al ser humano abordar lo absoluto.

La totalidad sólo ha podido ser alcanzable a través del ingenio humano para transgredir sus limitaciones físicas. La totalidad sólo es patente y asequible a través del artificio humano, de la Red de redes, de una conjunción de nodos que, interconectados, unifican los infinitos fragmentos de la totalidad y la hacen circular de manera enredada, para que el *todo* alcance simultáneamente a cada una de sus partes y éstas compongan simultáneamente la totalidad. Por eso la interacción virtual se impone a la física, porque nos hace sentir poderosos, *deidades* capaces de alterar los límites espacio-temporales y de alcanzar la totalidad de la que nuestra naturaleza humana aparentemente nos privaba.

La realidad palpable ya no nos satisface, ya no es suficiente, porque nos limita. El cara a cara ahora es un *peer to peer* vía Skype que transgrede los límites espaciales; las conversaciones más vehementes se trasladan del bar a Twitter; algunas revueltas

sociales abandonan los espacios secretos y se planean en público por obscenos exhibicionistas neoactivistas a los que las masas aplauden en un gran cabaret, mientras los hacktivistas contemplan atónitos esta exposición pública de la privacidad y el desprecio por el anonimato; el grado de obscenidad de la exposición pública de personajes famosos de la cultura popular de masas en Twitter y Facebook supera al de sus relatos de vida y su exhibicionismo en revistas y programas de televisión del *corazón*; los políticos adaptan la oratoria al nuevo laboratorio de pensamiento breve y fugaz que es Twitter, que nada tiene que ver con la valiosa y rentable tradición histórica del aforismo, el proverbio y el refrán que cultivaron los eruditos desde tiempos inmemoriales.

En este nuevo espacio de relaciones a distancia construimos las identidades de seres obscenos que se exhiben y se sobreexponen en el espacio público. Es lo que Baudrillard llama el éxtasis obsceno de la comunicación: "La obscenidad empieza cuando […] todo se vuelve transparente y visible de inmediato, cuando todo queda expuesto a la luz áspera e inexorable de la información y la comunicación" (Baudrillard, 1985: 193).

Las redes sociales y los blogs son amplificadores de opiniones, intereses, tendencias, obsesiones, afectos y manías personales. Exhiben el lado oculto que todos tenemos y guardábamos en los espacios privados y que ahora mostramos en público. Nuestras pasiones, nuestros sentimientos y emociones, nuestras frustraciones, nuestras preocupaciones, algunas opiniones sensibles y todo aquello que formaba parte de nuestra intimidad y privacidad o que no pasaba más allá de nuestros círculos más cercanos, hoy lo estamos volcando en la nueva esfera pública. Un blog y un perfil en Twitter o Facebook es un desnudarse ante el mundo, es algo *obsceno*. Es, en definitiva, la perversión de la realidad *trans*, de la indiferenciación entre lo público y lo privado, entre lo interno y lo externo, y en la que todo se hace visible en una doble obscenidad: "[…] los procesos más íntimos de nuestra vida se convierten en el terreno virtual del que se alimentan los medios de comunicación", pero también "todo universo llega a desplegarse arbitrariamente en nuestra pantalla doméstica" (Baudrillard, 1985: 193).

Es así como se legitima la función de vigilancia y sus gratificaciones (McQuail, Blumler, Brown, 1972). Para tener la sensación de control del entorno, el

individuo debe exponerse en el nuevo dominio público y dejar rastros, a la vez que tiene que dejarse invadir por la totalidad. Así, el Gran Hermano es la suma de muchos vigilantes; es el resultado de millones de *Grandes Hermanos* que, aceptando y normalizando su rol de vigilantes vigilados, legitiman al gran vigilante y sus estructuras discursivas de dominación.

III.6.1. #TuiteaUnSecreto: la obscenidad de quien ya no tiene vida privada, el éxtasis de la comunicación, la esquizofrenia colectiva

Frente a la apología tecnocomercial de las redes sociales *online* y los redundantes panegíricos de los nuevos mercaderes y augures de la comunicación, creemos necesario que se active y articule un discurso crítico sobre los medios sociales en línea. No vamos a negar los evidentes beneficios sociales —e individuales— que reportan las redes sociales; tampoco vamos a impugnar las ventajas y rendimientos que proporcionan. Sin embargo, la lectura crítica de las redes sociales en línea, o para ser precisos, del uso que hacemos de ellas y los efectos específicamente sociales y personales que de ese uso se derivan, merece estar no sólo en el centro del debate científico en ciencias de la comunicación y la información aplicadas al estudio de Internet como metamedio, también tiene que estar en el debate público.

El pensamiento crítico sobre los procesos sociales en las redes sociales *parece* marginado en el debate popular —tal vez por *incompatibilidad* con la propia dinámica mercantilista de las redes– y aislado en espacios científicos y marginales, desde donde apenas afecta o influye en el proceso de formación y configuración de una opinión pública crítica e ilustrada en la ética de la Red, la nética en Himanen (2001).

Desde una perspectiva científica, pero también desde la de una amplia experiencia profesional en el campo de la comuniación, uno de los aspectos que más nos ha preocupado en los últimos tiempos sobre los medios y las redes sociales *online*, es precisamente el de la renuncia voluntaria de los individuos a su privacidad, a su intimidad. Este es un problema que se puede abordar desde diversos enfoques concurrentes, por ejemplo: la cesión voluntaria de datos personales a corporaciones transnacionales a cambio del uso *gratuito* de herramientas *online*; el ejercicio de informarse como mecanismo de suministro de información personal a recolectores y traficantes de datos (*data brokers*), a través del *feedback* que generamos al navegar por

Internet; la aceptación y normalización del Estado de vigilancia, donde nuestra actividad *online* es monitorizada y analizada, y nuestros datos personales son registrados en enormes bases de datos de las que se sirven empresas y gobiernos para controlarnos (control en su más amplia acepción, no sólo dominio, también comprobación, inspección, fiscalización, intervención, regulación); o la exhibición y sobreexposición pública y *voluntaria* de lo privado, de lo íntimo, en un éxtasis comunicacional de las masas. Precisamente, sobre este último problema, que se manifiesta día a día en las redes sociales, encontramos un caso paradigmático en Twitter: un pacto social para la revelación del secreto personal a cambio de otros secretos ajenos.

El 24 de septiembre de 2013, el *hashtag* #TuiteaUnSecreto lideró la lista de *trending topics* en España y se viralizó por medio mundo; una demostración de que las redes sociales en línea nos están convirtiendo en seres con vidas de dominio público mediante una suerte de pacto social que empuja la voluntad propia al abismo de la transparencia de la vida privada y a la vulnerabilidad del individuo; nuestras vidas transfiguradas en bienes demaniales.

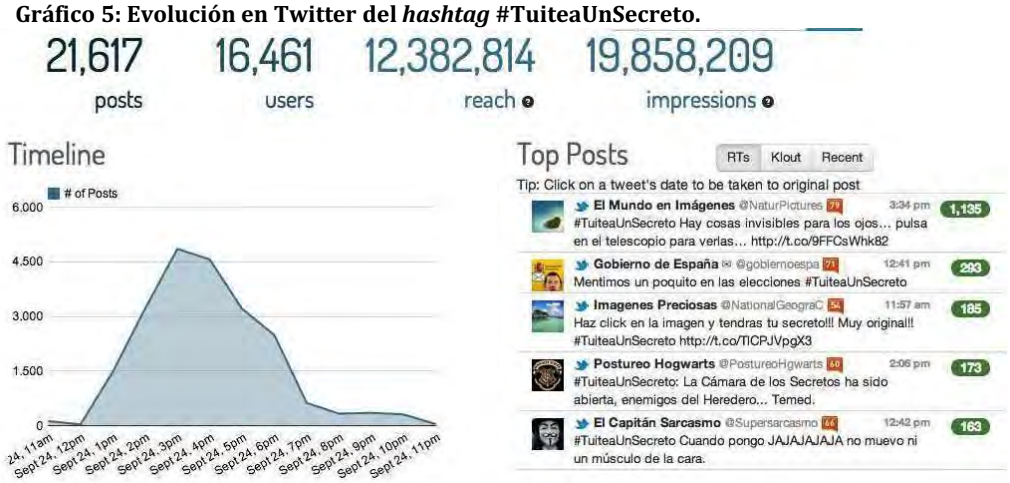
Cuadro 6: *Trending topics* en Twitter el 24 de septiembre de 2013.

Fuente: Twitter.

Más de 16.000 participantes, más de 21.000 *tweets*, más de doce millones de usuarios únicos alcanzados y casi veinte millones de impactos potenciales. Son las colosales cifras que logró sólo en sus primeras doce horas de actividad

el *hashtag* #TuiteaUnSecreto, según los datos que obtuvimos utilizando la herramienta de análisis Keyhole[109], que nos permite rastrear conversaciones en Twitter sobre un tema determinado.

Gráfico 5: Evolución en Twitter del *hashtag* #TuiteaUnSecreto.



Fuente: elaboración propia usando Keyhole.com.

En el nuevo espacio de relaciones virtuales a distancia y en red se construyen las identidades de seres que se exhiben y se sobreexponen en una *obscena* y *esquizofrénica* transparencia de sus vidas. En Baudrillard, obsceno es lo que acaba con toda mirada, con toda imagen, con toda representación.

> […] ya no es la tradicional obscenidad de lo que está oculto, reprimido, prohibido o es oscuro; por el contrario, es la obscenidad de lo visible, de lo demasiado visible, de lo más visible que lo visible. Es la obscenidad de lo que ya no tiene ningún secreto, de lo que se disuelve por completo en información y comunicación (Baudrillard, 1985: 194).

Obscena es, por lo tanto, esta nueva *pornografía* de la información y la comunicación, de los circuitos y las redes. Obscenidad pública que nos lleva a un estado de esquizofrenia colectiva, compartida, aplaudida, civilizada.

> [...] tendremos que sufrir este nuevo estado de cosas, esta extroversión forzada de toda interioridad, esta inyección obligada de toda exterioridad que significa literalmente el imperativo categórico de la comunicación. También aquí tal vez sea posible utilizar las viejas metáforas de la patología. Si la histeria era la patología de

[109] Keyhole es un servicio *freemium* que nos permite comprender cómo se produce y evoluciona un acontecimiento en Twitter en un momento determinado. Disponible en: http://keyhole.co/ (último acceso: 12 de diciembre de 2015).

> escenificación exacerbada del sujeto, una patología de la expresión, de la conversión teatral y operística del cuerpo; y si la paranoia era la patología de la organización, de la estructuración de un mundo rígido y celoso, entonces, con la comunicación y la información, con la promiscuidad inmanente de todas esas redes, con sus conexiones continuas, ahora nos encontramos en una nueva forma de esquizofrenia. No más histeria, no más paranoia proyectiva, propiamente hablando, sino este estado de terror propio del esquizofrénico: demasiada proximidad a todo, la sucia promiscuidad de todo cuanto toca, sitia y penetra sin resistencia, sin ningún halo de protección privada, ni siquiera su propio cuerpo, para protegerle.
>
> El esquizofrénico queda privado de toda escena, abierto a todo a pesar de sí mismo, viviendo en la mayor confusión. Él mismo es obsceno, la obscena presa de la obscenidad del mundo. Lo que le caracteriza no es tanto la pérdida de lo real, los años luz de separación de lo real, el pathos de distancia y separación radical, como suele decirse, sino, muy al contrario, la proximidad absoluta, la sensación de que no hay defensa ni posible retirada. Es el fin de la interioridad y la intimidad, la excesiva exposición y transparencia del mundo lo que le atraviesa sin obstáculo. Ya no puede producir los límites de su propio ser, ya no puede escenificarse ni producirse como espejo. Ahora es sólo una pura pantalla, un centro de distribución para todas las redes de influencia (Baudrillard, 1985: 196-197).

Una esquizofrenia viral que circula y se contagia por las redes de comunicación a todo el mundo, como un apocalipsis zombi.

Ilustración 17: Impacto geográfico del uso del *hashtag* #TuiteaUnSecreto.

Fuente: elaboración propia usando Keyhole.com.

III.7. UNA NUEVA DROGA: INFLUENCIA Y REPUTACIÓN ONLINE

Ya hemos visto que la atención de los otros es la más irresistible de las drogas en la realidad líquida de la sociedad red. En este sentido, las herramientas de monitorización y visualización han contribuido a ponderar y reafirmar el papel relevante que los líderes de opinión —los usuarios que mayor visibilidad y atención reciben— juegan como intermediarios entre los medios de comunicación y los ciudadanos. Hoy, todo cuanto sucede en Internet es medible y cuantificable, no sólo el tráfico web de referencia, orgánico y directo, las páginas vistas y los usuarios únicos, el promedio de tiempo en el sitio web, las características demográficas de los usuarios, los navegadores y dispositivos que utilizan, de dónde vienen y adónde van, la masa de seguidores en redes sociales, el número de *retweets* o las veces que una información ha sido compartida en Facebook. Hoy es tan importante medir todo esto como ponderar la influencia y reputación, indicadores de nuestra visibilidad e impacto en la Red de redes, y, por lo tanto, fundamentales en esta nueva lógica económica en la que la atención es la moneda de cambio, la medida de todas las cosas. Medidores públicos de la reputación e influencia *online* como Klout, Kred o PeerIndex se han convertido en la nueva droga de los usuarios de redes sociales y coadyuvan a establecer jerarquías de poder, a conceder estatus, a otorgar popularidad y a gratificar a los usuarios con premios en forma de puntuaciones y ránkings.

Influir nunca ha gratificado tanto como ahora. Así, en Twitter, Facebook, Google Plus, LinkedIn o YouTube ya no basta la mera cuantificación de seguidores, amigos, fans o votos para enjuiciar la relevancia. Variables como el número de seguidores activos, el contenido redistribuido o comentado, y el grado de relevancia de las cuentas que interaccionan con uno, se entrecruzan para determinar cuán importante se es en la web social. En un entorno saturado, en el que sobreabundan perfiles y relatos, parece importante medir la capacidad que empresas, administraciones, instituciones, organizaciones e individuos tienen para hacer impactar sus mensajes en los *otros*. La medición, mediante algoritmos de software, de la capacidad de influir y de captar atención se ha convertido en la nueva forma de jerarquización social.

Contra la tesis de Ramón Trecet (2011), un usuario no sólo vale, en términos de influencia, su número de seguidores en redes sociales; la cifra es importante sólo en apariencia. Por ejemplo, seguir y ser seguido por veinte mil usuarios no garantiza

relevancia en Twitter; son las interacciones y respuestas que se reciben las que verdaderamente cuantifican y cualifican la importancia de un usuario: alguien con dos mil seguidores, entre los cuales ha logrado fidelizar y crear una comunidad que le respalde activamente, puede generar más tráfico a su página web y más menciones en Twitter y en otros canales web, que aquél que ha conseguido sumar un número de seguidores diez veces mayor, pero en su mayoría pasivos o durmientes. Por tanto, la credibilidad e influencia, si se pueden cuantificar, no dependen tanto del número de seguidores como de la cantidad y calidad del *feedback* y de las acciones que se generan, dentro y fuera de Twitter. De lo que se trata es de dar valor a los usuarios activos entre los muchos seguidores pasivos o durmientes. Lo sustancial es la cuantificación del *feedback* para medir la reputación e influencia *online*: calcular cuántos de esos seguidores son realmente usuarios activos en Twitter o Facebook, cuántos son pasivos o durmientes, cuántos interaccionan y qué volumen de *replies*, *retweets*, recomendaciones, *followfriday* (#FF), *trends*, favoritos, "me gusta" y clics en las URL compartidas generan los seguidores.

La figura de los *influencers* adquiere, pues, un papel clave en el nuevo ecosistema comunicativo. Entre los medios de información y los ciudadanos encontramos una nueva casta de líderes de opinión, los influyentes de las redes, mediadores entre las estructuras discursivas de dominación de los grupos de poder tradicionales y los ciudadanos en los que impactan sus mensajes, actualizando el enunciado de Bernard Cohen: "La prensa no tiene mucho éxito en decir a la gente qué tiene que pensar pero sí lo tiene en decir a sus lectores sobre qué tienen que pensar" (Cohen, 1963: 13). Este rol ahora lo comparten con los nuevos *influencers* de las redes.

Los *influencers* no sólo actúan como *gatekeepers*, —desde sus blogs, sus espacios de opinión conquistados en los medios de información o sus perfiles en redes sociales—, decidiendo qué es relevante y qué no lo es, determinando qué temas merecen ser redistribuidos y sobre cuáles debemos pensar y discutir; también suelen actuar como los nuevos cabilderos que pretenden influir en las decisiones de gobiernos, empresas y medios. Buen ejemplo de ello en España es el papel que jugaron algunos denominados *gurús* de Internet en el intento de hacer fracasar la Ley

Sinde en España, diseñada para regular las descargas en Internet[110]. La masiva movilización ciudadana, promovida por periodistas, abogados y tecnólogos influyentes, puso contra las cuerdas al Gobierno socialista de José Luis Rodríguez Zapatero, generando importantes disensiones en el Ejecutivo español y un enardecido debate público entre partidarios del *copyright* y defensores de una Internet libre de las viejas normas de la sociedad industrial. Aquél se recuerda como el mayor y más caliente debate público que ha habido en España hasta ahora sobre libertades y derechos en la Red.

Un *influencer* puede movilizar a las masas contra un gobierno o una ley. Pero también puede, por ejemplo, influir en la compra de un producto, ayudar a arruinar la imagen de una marca o empresa, o intentar dirigir el voto en un proceso electoral. Sin embargo, esta capacidad de coacción sobre los poderes tradicionales, y de influencia sobre los usuarios, es sólo una aproximación adulterada a la democracia participativa que se pretende. Aproximación aparente a la democracia participativa por la intervención, precisamente, de nuevas elites, nuevos líderes de opinión y grupos de presión que ejercen un poder bidireccional: por un lado, hacia los ciudadanos usuarios de la Red, reprimiendo su capacidad librepensadora al establecer los temas de la agenda pública y pautando las reacciones a éstos; y por otro lado, hacia gobiernos, empresas, instituciones y medios de comunicación, a los que coaccionan con su capacidad de movilizar a los usuarios de la Red y de crear climas de opinión por contagio masivo, según convenga, de manera que el resultado es un proceso en espiral en las redes sociales que incita a los otros a percibir los cambios de opinión y a seguirlos hasta que una opinión se establece como la actitud prevaleciente (Noelle-Neumann, 1974).

Los vínculos de los *influencers* con su comunidad de fieles se sostienen en una confianza afectiva, canalizada en las redes sociales en línea. El *retweet* en Twitter o el clic en "me gusta" y "compartir" en Facebook lo que hacen, en el caso de los seguidores fieles, es viralizar esa empatía, que a veces deriva en cuestión de fe. Hay un fenómeno que venimos observando desde hace tiempo en Twitter, en nuestra experiencia profesional, que es lo que llamamos un "*retweet* autómata" o

[110] La Ley Sinde es el nombre popular con el que se conoce una disposición de la Ley 2/2011 , de 4 de marzo, de Economía Sostenible, para regular Internet en España y proteger el derecho de propiedad intelectual.

"automatizado", que es el que se produce cuando un usuario *retuitea* un enlace compartido por uno de sus *influencers* sin haber leído el contenido que se enlaza. En los casos de los blogueros, artistas, periodistas y medios más influyentes en Twitter, se observa como algo habitual: comparten en Twitter un *post* con un enlace a un texto o a un vídeo que pueden llevar tres, cuatro, cinco minutos leerlo o verlo, a veces más, pero muchos de sus fieles y fervientes seguidores, como obnubilados por una cuestión de fe, *retuitean* y comparten esa URL inmediatamente, escasos segundos después de saltar a Twitter el *post* original, sin haber tenido tiempo de leer el texto o de ver el vídeo compartidos. Parece un comportamiento irreflexivo, compulsivo, autómata, que bien merece un estudio científico para determinar los niveles de influencia de los líderes de opinión en las redes sociales, los comportamientos que generan en sus seguidores, los tipos de vínculos que se establecen y el impacto real de los contenidos que comparten.

Esta relevancia de los nuevos líderes de opinión ha hecho que las empresas del sector de la comunicación sean cada vez más conscientes de que para alcanzar en las redes sociales a las multitudes, primero deben identificar a los *influencers* y crear un vínculo de confianza para, a través de ellos, hacer crecer exponencialmente el mensaje en las redes (se crea una cadena jerárquica: el *influencer* filtra el contenido del medio que considera debe estar en la agenda pública; otro usuario influido por el líder de opinión se lo filtra a un tercero que, por empatía, se fía de este, y así sucesivamente). Varios estudios ya han demostrado que son los *influencers* quienes generan en las redes sociales la mayor parte de contenidos que luego viralizan el resto de usuarios, obnubilados por estas nuevas elites.

El estudio 'Who Says What to Whom on Twitter', presentado en 2011 en la 20th Annual World Wide Web Conference, en Hyderabad (India), analiza los patrones de comportamiento de los usuarios de Twitter en Estados Unidos. Los resultados sobre la producción, flujo y consumo de la información en esta red social ponen de manifiesto que una elite que representa apenas el 0,05 por ciento de los usuarios de Twitter publica el 50 por ciento de las URL compartidas y es la que recibe mayor atención en esta red social. Esta elite está formada por celebridades, blogueros influyentes y representantes de medios de información dominantes y de otras organizaciones con poder real, y que se distinguen de lo que los autores del estudio

llaman "usuarios ordinarios". La investigación revela que si bien son los medios de comunicación los que producen la mayor cantidad de información, las cuentas de las celebridades son las que acaparan un mayor número de seguidores.

Por otro lado, los investigadores encuentran un comportamiento endogámico significativo entre los distintos grupos identificados como elites. Así, las celebridades escuchan a las celebridades; los blogueros relevantes atienden casi exclusivamente a otros blogueros influyentes, etc. Y entre esas elites, son los blogueros los que más información redistribuyen. Además, casi la mitad de la información que se genera en los medios de comunicación impacta en las multitudes indirectamente a través de los filtros de los líderes de opinión, que están más conectados y expuestos a los medios que el resto de usuarios, según este estudio. Así, la atención que antes estaba restringida a los medios de información de masas ahora se comparte con estas elites, lo cual condiciona las estrategias de los medios en las redes sociales, siendo para éstos fundamental identificar a los *influencers* que trasladarán los contenidos a los ciudadanos.

Lazarsfeld sigue vigente, quizá más que nunca. La Teoría de los dos pasos (1955) encuentra perfecto acomodo en esta nueva realidad comunicativa de ilusiones horizontales, en la que la influencia personal de los usuarios *top* intermedia entre los mensajes de los medios y las decisiones de las personas. Por eso, cada vez más es importante lograr la confianza, o al menos la atención e interés, de esos *influencers*, que son los todopoderosos intermediarios. Porque, contra el discurso de muchos ingenuos, el poder de los intermediarios, en todos los niveles, es evidente en Internet, en general, y en las redes sociales, en particular. Lo que sucede es que aparecen nuevos intermediarios.

Para completar esta visión recurrimos a la investigación *Trends in Social Media: Persistence and Decay*, realizado por investigadores del Laboratorio de Computación Social HP Labs, en Palo Alto, y el Departamento de Física Aplicada de la Universidad de Stanford. Sus autores llegan a la conclusión de que los *trending topics* de Twitter —los temas más populares— son, en un gran número, noticias procedentes de los medios tradicionales y amplificadas con sucesivos *retweets* para acabar generando los *trends* (tendencias) en Twitter. Según los resultados obtenidos por los investigadores, "los medios de comunicación social, lejos de ser una fuente

alternativa de noticias, funcionan más como un filtro y un amplificador de noticias de interés de los medios tradicionales" (Asur, Huberman, Szabo y Wang, 2011. Es decir, contra el mito de la horizontalidad y de la desintermediación, el emisor institucional mantiene su poder e influencia, y ahora se ve amplificado por los *retweets* y la ubicuidad. Se vuelve así humo lo que pensamos era parte de los grandes avances de Internet: permitir una configuración horizontal de las relaciones sociales, rompiendo los nervios de los centros de poder. Los medios tradicionales siguen, directa e indirectamente, impactando a las masas —ahora transfiguradas en multitud— y continúan en los nuevos canales su tradicional labor de *iluminar* a sus públicos, aunque ahora deben hacerlo con especial atención a los *influencers* capaces de canalizar sus mensajes hacia los ciudadanos. En consecuencia, el emisor sigue importando mucho.

III.8. LOS HIPERMERCADOS DE LA INFORMACIÓN

Llegados a este punto, se nos antoja apropiado traer y adaptar a este escenario un texto de Michel Houellebecq para concluir esta reflexión sobre la era de la transrealidad y la sociedad que existe en red; de la aberración de lo *glocal*; de la inestabilidad y mutabilidad del ser paradójico que se siente libre alimentando el control de los medios de comunicación tradicionales y de las megacorporaciones transnacionales; del individuo que renuncia a la remuneración económica no por un principio ético sino por conseguir una sobredosis de atención; de los medios que abandonan su papel de productores de información de interés general y se lanzan progresivamente a su transformación en enormes agregadores de opiniones de líderes sociales y de relatos efímeros, de historias fugaces para un modelo de mínimos costes y máxima rentabilidad para el capitalismo tecnológico, en el que la supremacía de la cantidad y el consumo continuo e incesante de relatos fugaces acarrea un abandono de la calidad, de la profundidad y de la reflexividad que requiere la producción, consumo y uso de la información. Es el mundo como hipermercado de la comunicación y de la información[111], el de una oferta, demanda y consumo masivos de la información como mercancía, con la que se trafica en un espectáculo global que induce forzosamente a la dispersión de nuestros sentidos. Es la actualización de *El mundo como supermercado y como burla* de Houellebecq, ahora convertido en hipermercado:

> El hombre de supermercado no puede ser, orgánicamente, un hombre de voluntad única, de un solo deseo. De ahí viene cierta depresión del querer en el hombre contemporáneo; no es que los individuos deseen menos; al contrario, desean cada vez más; pero sus deseos se han teñido de algo un tanto llamativo y chillón; sin ser puros simulacros, son en gran parte un producto de decisiones externas que podemos llamar, en sentido amplio, publicitarias. No hay nada en esos deseos que evoque la fuerza orgánica y total, tercamente empeñada en su cumplimiento, que sugiere la palabra «voluntad». De ahí se deriva cierta falta de personalidad, perceptible en todos los seres humanos (Houellebecq, 2000: 65).

En el supermercado de la comunicación y de la información, o más precisamente, hipermercado, cuyos paradigmas son Facebook (redes sociales) y *The Huffington Post* (medios de información), se produce la aceleración de las

[111] Hemos revisado y cambiado el concepto original del supermercado de la información que adelantamos como parte de esta investigación en el *paper Supermercados de la información en la era de la transrealidad*, publicado en la revista *Versión. Estudios de Comunicación y Política*, editada por la Universidad Autónoma Metropolitana Unidad Xochimilco, México. Consideramos que el concepto de hipermercado se ajusta mejor en nuestra interpretación actualizada.

percepciones y de las sensaciones que caracteriza a la lógica del hipermercado y del hiperconsumo (Lipovetsky, 2006), contraria a la pausa y la reflexión:

> No hay lectura sin parada, sin movimiento inverso, sin relectura. Algo imposible e incluso absurdo en un mundo donde todo evoluciona, todo fluctúa; donde nada tiene validez permanente: ni las reglas, ni las cosas, ni los seres (Houellebecq, 2000: 67).

La información ahora se expande en el infinito del ciberespacio a la velocidad de la luz. Su instantaneidad e inmediatez impiden la profundidad del escritor y la reflexividad del lector, ahora abrumado por un *continuum* de nuevos contenidos y mensajes que van excluyendo a sus predecesores a un ritmo desenfrenado; esta fugacidad los envía al olvido por ese suceder constante de *noticias* que lo convierte todo en anecdótico:

> A causa de la explosión de la información, ya no leemos, ojeamos. Las noticias que se usaban durante un día ahora sólo duran un par de horas, simplemente porque tenemos que prestar atención a las noticias nuevas. Por lo tanto, es cada vez más difícil manejar todas las fuentes de noticias y mantenerse en la cima de las cosas. Lo que nos lleva a la ley de información enunciada por primera vez por Herbert Simon: el rápido crecimiento de la información provoca falta de atención (Iskold, 2007).

La actualización permanente, el presente continuo y acelerado, resulta de la suministración constante de productos informativos por parte de una masa de nuevos autores, consumidores transfigurados en productores que colaboran en la manufacturación a gran escala de productos informativos o de entretenimiento personalizados (McLuhan y Nevitt, 1972; Toffler, 1980) para nutrir a la larga cola, pero también a la cabeza del mercado, a cambio de atención. Esta producción a gran escala facilita que los reponedores mantengan las góndolas de los hipermercados de la información óptimamente abastecidas y se aseguren que haya siempre mercancía nueva disponible para el hiperconsumo en un hiperespacio saturado de productos extremadamente perecederos y en el que un minuto de visibilidad y atención es sinónimo de éxito. Así, los prosumidores, en su doble rol de hiperproductores e hiperconsumidores, aseguran la supervivencia de los grandes hipermercados del entretenimiento: YouTube, Amazon, Facebook, etc., pero también favorecen, en el sector del periodismo, el nuevo modelo de negocio de la agregación o integración masiva y a bajo coste de información generada por los prosumidores, y cuyo máximo

exponente es el modelo de *The Huffington Post*.

La información ha sido cosificada para la cultura del espectáculo de tal manera, que apenas podemos distinguirla ya de un producto de entretenimiento del capitalismo tecnológico como el iPhone. La información hoy es diseñada como mercancía para la nueva cultura hiperconsumista, programada para una cada vez más acelerada obsolescencia, vendida como producto del desarrollo tecnológico y repuesta una y otra vez para generar millones de interacciones que sirvan como argumento de venta.

Experimentamos en un simulacro la utopía de un mundo de iguales y horizontal. Pero la realidad es que Internet se recentraliza en torno a unos pocos nodos de control que concentran los beneficios económicos y los principales resortes de la Red, reedificando un nuevo poder más centralizado que se alimenta del *feedback* de los usuarios: consagramos el *feedback* como cáliz de la salvación y ofrecemos a las elites nuestro *ADN* digital en los puntos de control de las estructuras panópticas del poder. Es, de nuevo, la paradoja del control. *Facebook macht frei*.

Así, los grandes hipermercados de la información y del entretenimiento concentran los beneficios económicos, pero también ejercen poder de influencia y concitan la atención de las masas; estos dos valores simbólicos los comparten, el primero con los líderes de opinión que actúan como intermediarios entre los medios y los ciudadanos a los que influyen, y el segundo, con los usuarios ordinarios cuyos egos son gratificados con la atención por los servicios prestados como productores de contenidos.

El objetivo sigue siendo el de siempre, pero ahora compartido, aunque con réditos distintos: impactar al máximo número de receptores y vendernos lo que sea, como sea, cuando sea y donde sea. Lo que pasa es que ahora la nueva realidad hiperfragmentada obliga a rediseñar y pulir las estrategias de comunicación en un entorno que apenas estamos empezando a conocer, que muta a una velocidad endiablada y en el que los resultados de las acciones emprendidas nunca son concluyentes debido a la inestabilidad y permanentes transformaciones del nuevo ecosistema. Para entender esto no hay mejor medida que la incertidumbre generada en la que se mueven, y se reconocen, los expertos y empresas de comunicación, desconcertados y atosigados por esta nueva realidad líquida variable, voluble, mutable (Bauman, 2007), en la que, al menos en el sector periodístico, parece que aún nadie ha

encontrado la solución a los problemas y retos que deben resolver las empresas informativas en la sociedad red, no sólo los relativos a su sostenibilidad económica, sino, y sobre todo, a su ética.

La soberanía del hombre está oculta en el conocimiento.

—Francis Bacon.

IV. CASO DE ESTUDIO: WIKILEAKS

IV.1. ORÍGENES Y CRONOLOGÍA DEL FENÓMENO WIKILEAKS: OCTUBRE 2006 – DICIEMBRE 2010

La organización de filtraciones WikiLeaks nació el 4 de octubre de 2006, día en el que se registró el dominio wikileaks.org, según consta en la base de datos de la ICANN (Internet Corporation for Assigned Names and Numbers). Es importante subrayar que la elección del identificador *.org* denota la intención de Julian Assange y de sus colaboradores de dotar a su proyecto de una dimensión social, no comercial ni lucrativa.

El sufijo *.org* suele ser utilizado por organizaciones sin ánimo de lucro, organizaciones no gubernamentales, asociaciones, organizaciones supranacionales como la ONU y también por proyectos comunitarios de software libre y conocimiento compartido, como OpenOffice.org o Wikipedia.org, en oposición al identificador comercial *.com*, el más extendido en Internet, cuyo uso masivo da una idea clara de la tendencia mercantilista que impera en la Red. A fecha 3 de octubre de 2015, DomainTools —un servicio de análisis forense especializado en crímenes y amenazas en el ciberespacio, proveedor de información sobre registros web y datos DNS (Domain Name System)— contabilizaba 120.090.408 dominios *.com* (comercial), 15.056.015 *.net* (redes y proveedores de servicios de Internet), 10.648.489 *.org* (organizaciones y asociaciones) y 5.156.764 *.info* (informativo)[112]. Estos son los principales dominios de nivel superior genéricos y sin restricciones, es decir, aunque el sufijo —de tres o más caracteres— denota la naturaleza para la cual fueron creados, se permite su uso para cualquier propósito y por cualquiera persona física o jurídica. Los dominios territoriales también son de primer nivel y se caracterizan por terminaciones de dos letras

[112] Datos obtenidos de http://icannwiki.com/Domain_Statistics (último acceso: 3 de octubre de 2015].

identificativas de países o territorios (por ejemplo: *.es* para España; *.uk* para Reino Unido; *.fr* para Francia; *.us* para Estados Unidos, *.gal* para Galicia, *.cat* para Cataluña, etc.).

La elección del dominio *.org* para WikiLeaks clarifica su esencia: no se trata de un proyecto con ánimo de lucro ni quiere ser identificado como un mero servicio de información; WikiLeaks es una organización que presta un servicio público, que no es otro que liberar información confidencial y secreta de interés general, contribuir al ideal de transparencia en gobiernos y corporaciones, y defender los derechos humanos en todo el mundo.

Otro detalle importante en la fundación de WikiLeaks es que su dominio en Internet no fue registrado a nombre de Assange, sino de su padre biológico, John Shipton, y de su padre político *cypherpunk*, John Young, arquitecto y ciberactivista estadounidense que en 1996 creó junto con su esposa, y también arquitecta, Deborah Natsios, el sitio web de filtraciones Cryptome.org, antecedente de WikiLeaks.

Assange conocía a Young de la lista *Cypherpunks*, en la que estaban, entre otros muchos conocidos ciberlibertarios, John Gilmore, Eric Hughes, Timothy C. May, Jude Milhon, Jacob Appelbaum o Suelette Dreyfus. En enero de 2007, Young publicó en Cryptome.org las conversaciones que había mantenido con Assange y sus primeros colaboradores en una lista de correo creada para planear el lanzamiento de WikiLeaks[113].

En un correo electrónico enviado a Young el 3 de octubre de 2006, Assange propuso al arquitecto ser el registrador de un nuevo sitio web de "filtraciones masivas de documentos que necesita que alguien con agallas respalde el registro del dominio *.org*", cuyas normas exigen que los datos del registrador no sean falsos o engañosos. Assange ya anticipa entonces que ese dominio estaría "bajo la habitual presión política y legal" y que podría ser fácilmente cancelado, salvo que "alguien estuviese dispuesto a levantarse y a declarar ser el registrador"; una persona que no tendría que "declarar ningún otro conocimiento ni participación" en el proyecto (WikiLeaks Leak, 2007). Young aceptó y pasó también a formar parte del primer consejo asesor de WikiLeaks.

[113] Todas las citas tomadas de estas conversaciones son traducciones propias de los correos electrónicos originales, en inglés, publicados en Cryptome.org como *WikiLeaks Leak* y *WikiLeaks Leak 2* , el 7 y el 9 de enero de 2007, respectivamente.

Cuadro 7: Registro del dominio wikileaks.org, el 4 de octubre de 2006

```
Domain Name:WIKILEAKS.ORG (etc)

Created On:04-Oct-2006 05:54:19 UTC

Last Updated On:04-Oct-2006 06:45:38 UTC
Expiration Date:04-Oct-2007 05:54:19 UTC
Sponsoring Registrar:Dynadot, LLC (R1266-LROR)
Status:TRANSFER PROHIBITED
Registrant ID:CP-10335
Registrant Name:John Young c/o Dynadot Privacy
Registrant Street1:PO Box 1072
Registrant Street2:
Registrant Street3:
Registrant City:Belmont
Registrant State/Province:CA
Registrant Postal Code:94002
Registrant Country:US
Registrant Phone:+1.6505851961
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:privacy@dynadot.com
```

Fuente: captura de pantalla propia tomada de http://cryptome.org/wikileaks/wikileaks-leak.htm (último acceso: 4 de octubre de 2015).

Sin embargo, desavenencias posteriores entre Assange y Young llevaron al segundo a desligarse por completo del proyecto WikiLeaks en enero de 2007. Young cuestionó tanto el modelo económico que Julian Assange había diseñado —su intención era conseguir cinco millones de dólares para asegurar la viabilidad del proyecto—, como la palabra del propia Assange.

En un duro mensaje enviado por correo electrónico a la lista de correo de WikiLeaks el 7 de enero de 2007, Young puso en entredicho la existencia de 1,2 millones de documentos que los miembros de esta nueva organización decían poseer (WikiLeaks Leak, 2007). En un segundo correo enviado ese mismo día, Young acusó a WikiLeaks de ser un instrumento de la CIA. Y ya en el último *email*, el fundador de Cryptome avisó a los participantes en esta lista de correo de que había iniciado la publicación de los mensajes allí vertidos para explicar públicamente cómo había sido "inducido a servir como ciudadano estadounidense" para el registro del dominio WikiLeaks.org.

John Young tachó a WikiLeaks de "fraude", de ser una "campaña de desinformación contra la legítima disidencia" y de "trabajar para el enemigo".

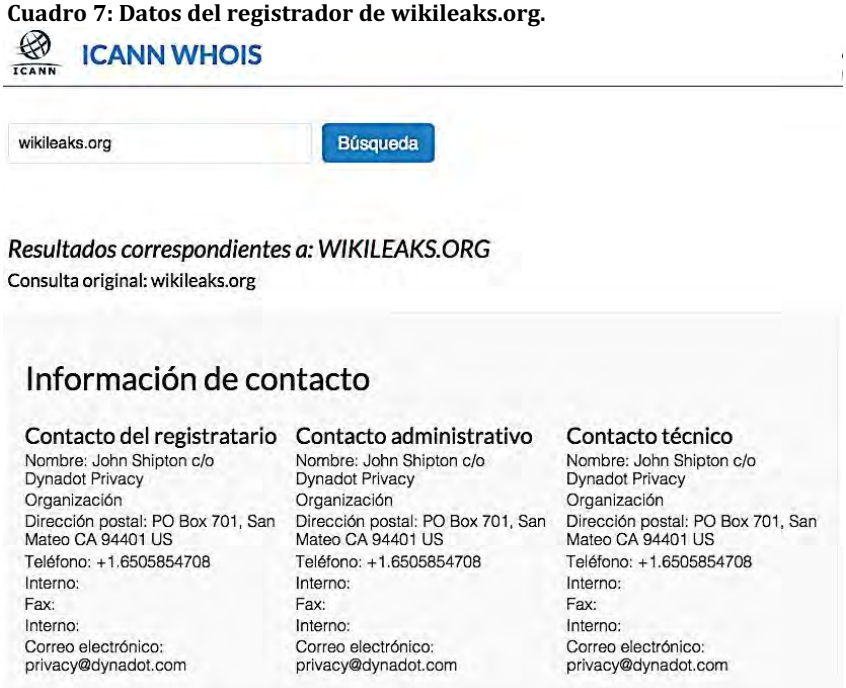
(WikiLeaks Leak, 2007). Con aquellos correos electrónicos, Young se despidió de WikiLeaks.

El fundador de Cryptome había empezado a especular con la idea de que WikiLeaks era una operación encubierta de la CIA. Éste ha sido uno de los rumores más difundidos por la Red para desprestigiar a esta organización y a Julian Assange desde entonces. Pero nadie, hasta el momento, ha aportado pruebas de ello. A lo más que se ha llegado es a fantasear con esta idea basándose en especulaciones sobre la manera en que se financia WikiLeaks y su alianza con ciertos medios —en particular, con *The New York Times*, periódico acusado tanto por los críticos de WikiLeaks como, posteriormente por el propio Assange, de ser un instrumento al servicio del Gobierno de Estados Unidos y de elites económicas—, llevándonos a un extraño silogismo que ha pretendido ser la prueba de que WikiLeaks sirve a los intereses de la CIA: si *The New York Times* ha colaborado con la CIA y WikiLeaks ha colaborado con *The New York Times*, entonces WikiLeaks es un agente de desinformación para limitar y controlar formas de oposición que necesitan ser vehiculizadas por el Gobierno de Estados Unidos. Algunos críticos con WikiLeaks también han querido ver en la campaña contra esta organización en Estados Unidos —basada fundamentalmente en la Ley de Espionaje de 1917 (Espionage Act)— un intento deliberado de la CIA por justificar el la regulación y control de Internet.

En definitiva, los conspiranoicos han venido argumentando que WikiLeaks es una agencia de desinformación de la Agencia Central de Inteligencia de Estados Unidos, pero nadie, ni siquiera expertos en filtraciones de informaciones secretas, han aportado hasta el momento algún documento o cualquier prueba que lo corrobore. De hecho, el propio Young acabó cambiando de opinión sobre WikiLeaks y descartó que ésta fuese una organización al servicio de la CIA, aunque ha mantenido sus críticas a la manera en que ésta se promociona y a su capacidad para proteger sus fuentes (Symington, 2009).

Con John Young desligado de WikiLeaks, Julian Assange necesitaba otro registrador para el dominio en Internet del sitio web de la nueva organización de filtraciones. El elegido fue su padre biológico, John Shipton, cuyo nombre aún figura en los registros de la ICANN como la persona de contacto para el dominio wikileaks.org.

Cuadro 7: Datos del registrador de wikileaks.org.



Fuente: captura de pantalla propia tomada de http://whois.icann.org/ (último acceso: 4 de octubre de 2015).

En los orígenes de WikiLeaks, tan importante fue el registro del dominio como la elección del nombre para la organización. La raíz de éste tiene dos interpretaciones: *wiki* es un neologismo inglés que proviene de la expresión hawaiana *wiki-wiki*, cuyo significado es "rápido", pero adaptada al inglés, se le ha atribuido el significado de "sitio web cuyas páginas pueden ser editadas directamente desde el navegador, donde los usuarios crean, modifican o eliminan contenidos que, generalmente, comparten" (*Wiki*, 2015), definición que fue adoptada por el Oxford English Dictionary.

El primer sitio *wiki*, bautizado con el nombre WikiWikiWeb, fue lanzado el 25 de marzo de 1995 por el programador Ward Cunningham para el Portland Pattern Repository (repositorio de patrones de diseño de software). Según el propio Cunningham, "la belleza del *wiki* está en la libertad, simplicidad y poder que ofrece" (*WikiWikiWeb*, 2015). Seis años después, el 15 de enero de 2001, Jimmy Wales y Larry Sanger lanzaron un proyecto inspirado en el movimiento del software libre que consolidó los *wikis* como una nueva expresión de la inteligencia colectiva en la cultura popular: la Wikipedia.

Wikipedia es una enciclopedia digital políglota, colaborativa y gratuita que se

construye sobre un software de código abierto llamado MediaWiki. Ha sido definida por sus propios creadores como "la enciclopedia de contenido libre que todos pueden editar", lema que resume sus tres principios, explicados también en su sitio web: 1) "es una enciclopedia, entendida como soporte que permite la recopilación, el almacenamiento y la transmisión de la información de forma estructurada", 2) "es un *wiki*, por lo que, con pequeñas excepciones, puede ser editada por cualquiera" y 3) "es de contenido abierto" (Wikipedia, 2015). Para dar sentido a estos principios, Wikipedia adopta licencias libres que la colocan bajo el paraguas de la cultura hacker y la distancian de las restricciones impuestas por las normativas tradicionales sobre el derecho de autor expresadas en licencias privativas. Wikipedia permite que todos los textos e imágenes creados y publicados por los usuarios, así como su software, puedan ser copiados, modificados y redistribuidos por cualquier persona, con la única condición de que se reconozca la labor de los contribuidores y que no se impongan restricciones a las obras derivadas.

Esta enciclopedia libre inspiró conceptualmente el proyecto WikiLeaks, que nació pretendiendo ser una organización de filtraciones rápidas, pero también un sitio colaborativo en el que cualquier persona pudiese contribuir a la publicación y edición de documentos secretos. Sin embargo, aquellas primeras intenciones se corrigieron posteriormente para hacer de WikiLeaks una organización informativa en la que existen ciertos controles sobre los archivos antes de su liberación.

Desde finales de 2006, y hasta el año 2010, WikiLeaks fue mutando su naturaleza y estrategia en un proceso evolutivo marcado por su relación con los medios de información tradicionales. Daniel Domscheit-Berg, activista tecnológico alemán, excolaborador de Julian Assange entre diciembre de 2007 y septiembre de 2010, y fundador del sitio web de filtraciones OpenLeaks[114], aporta en su libro *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website* (2011) una cronología del fenómeno WikiLeaks desde sus orígenes hasta el 30 de diciembre de 2010, día en el que se presentó OpenLeaks como alternativa a WikiLeaks, en plena efervescencia de este fenómeno. Domscheit-Berg recopila los hitos y los eventos más destacados de los primeros cuatro años de actividades de esta

[114] Tras su salida de WikiLeaks, Domscheit-Berg registró el sitio de filtraciones openleaks.org en septiembre de 2010. El 26 de enero de 2011, el proyecto se declaró abierto a potenciales confidentes y organizaciones que creen en la transparencia informativa.

organización[115], decisivos en su transmutación y fundamentales para entender cómo WikiLeaks se convirtió en un actor inesperado en la esfera pública.

Cuadro 8: Cronología de la actividad de WikiLeaks entre octubre de 2006 y diciembre de 2010.

2006	4 de octubre	Se registra el nombre de dominio WikiLeaks.org.
	Diciembre	Primeros documentos publicados en el sitio web de WikiLeaks.
2007	Enero	WikiLeaks anuncia que tiene 1,2 millones de documentos esperando ser procesados y publicados.
	Noviembre	WikiLeaks publica documentos sobre abusos en el centro de detención de la base militar de Guantánamo.
	Diciembre	Daniel Domscheit-Berg conoce a Julian Assange en el 24 Chaos Communication Congress (24C3), organizado por el Chaos Computer Club en Berlín.
2008	Enero	WikiLeaks publica documentos obtenidos de la sucursal del banco suizo Julius Bär en las Islas Caimán, con una lista de clientes con cuentas opacas.
	Febrero	Julius Bär demanda a Dynadot (proveedor del alojamiento y del dominio de WikiLeaks.org), pierde la medida cautelar que obtuvo para cerrar el sitio Wikileaks y luego retira la demanda.
	Marzo	WikiLeaks publica los manuales de la Iglesia de la Cienciología.
	Mayo	WikiLeaks revela el primer manual de una fraternidad en Estados Unidos.
	Junio	WikiLeaks publica documentos del *Memorandum of Understanding*, un convenio entre el político keniano Raila Odinga y el National Muslim Leader's Forum del país africano.
		Assange y Domscheit-Berg acuden a la cumbre de Global Voices en Budapest.
	Septiembre	WikiLeaks publica correos electrónicos de la cuenta privada de Sarah Palin, candidata republicana a la vicepresidencia de Estados Unidos.
	Noviembre	WikiLeaks publica una lista con los nombres de miembros del British National Party, formación política de extrema derecha.
		WikiLeaks publica un informe de la Oscar Legal Aid Foundation sobre la política de asesinatos de la Policía keniata.
	Diciembre	WikiLeaks publica documentos del Servicio Secreto alemán sobre casos de corrupción en Kosovo y de colaboración con algunos medios de comunicación alemanes.
		WikiLeaks publica el manual del Human Terrain Team de 2008.[116]
		Daniel Domscheit-Berg y Julian Assange protagonizan su primera conferencia oficial en el Chaos Communication Congress (25C3).
2009	Enero	Daniel Domscheit-Berg deja su para a trabajar a tiempo completo en WikiLeaks.
	Febrero	WikiLeaks publica más de 6.700 documentos del Servicio de Investigación del Congreso de Estados Unidos.
		WikiLeaks publica por un descuido las direcciones de correo electrónico de los donantes de la organización.

[115] Nótese que se trata de una cronología en la que el autor destaca algunos hitos y eventos relacionados con su experiencia personal y su país de origen, Alemania.

[116] El manual detalla el programa *Human Terrain System* del Pentágono, desarrollado en la base militar de Fort Leavenworth (Kansas) para el Ejército de Estados Unidos. Según éste, los equipos del *Human Terrain System* incorporan en las unidades militares sobre el terreno a antropólogos y académicos en Ciencias Sociales, para que faciliten la relación con la población civil y contribuyan a un mejor conocimiento del entorno cultural por parte del mando operacional.

2009	Marzo		WikiLeaks publica la base de datos con los nombres de las personas que financian la campaña del senador republicano por Minnesota Norm Coleman[117].
	Abril		Los miembros de WikiLeaks participan en el Festival Internacional de Periodismo en Perugia, Italia.
	Junio		WikiLeaks recibe el Premio Amnistía Internacional en la categoría de Nuevos Medios.
	Julio		WikiLeaks publica una lista de los mayores deudores del Icelandic Kaupthing Bank[118].
	Agosto		Conferencia en el Hacking At Random[119] (HAR) de Vierhouten, en Holanda.
	Septiembre		WikiLeaks recibe el premio de Ars Electronica en la categoría Digital Communities.
	Octubre		WikiLeaks hace pública una segunda lista con más nombres de los miembros del British National Party, formación política de extrema derecha.
	Noviembre		WikiLeaks publica medio millón de mensajes de texto enviados en Estados Unidos el 11 de septiembre de 2001, antes, durante y después de los atentados terroristas.
			WikiLeaks publica las diligencias contra una compañía farmacéutica alemana.
			WikiLeaks saca a la luz los contratos de la compañía alemana Toll Collect[120].
			WikiLeaks publica la correspondencia por correo electrónico de David Irving[121].
			WikiLeaks participa en el desarrollo de la idea de un refugio seguro para medios de comunicación, periodistas y fuentes, que conduce a la Iniciativa Islandesa de Medios Modernos (IMMI) para convertir a Islandia en un espacio libre y seguro para el periodismo independiente y de investigación.
	Diciembre		WikiLeaks publica los informes de campo sobre el bombardeo de dos camiones de combustible en Kunduz, Afganistán[122].
		Día 23	WikiLeaks paraliza por primera vez sus actividades y pasa a un estado *offline*.
		Día 27	Daniel Domscheit-Berg y Julian Assange hablan del futuro de WikiLeaks en el Chaos Communication Congress (26C3).
2010	5 de enero		WikiLeaks empieza a colaborar en la Icelandic Modern Media Initiative.

117 Una rumorología ciberespacial apuntó al magnate George Soros como principal benefactor de WikiLeaks y director de esta operación contra Coleman. Según estas teorías, Soros quería como presidente del Banco Mundial a Mark Malloch Brown, mano derecha de Kofi Annan (exsecretario general de la ONU), al que se oponía Coleman. El demócrata Al Franken, respaldado por Soros, derrotó a Coleman.

118 WikiLeaks publicó documentos que revelaban cómo Hreidar Mar Sigurdsson, presidente del banco Kaupthing, había prestado varios miles de millones de euros a sus mayores accionistas y asociados sólo una semana antes de que el banco islandés fuese nacionalizado el 9 de octubre de 2008.

119 Hacking At Random es un festival internacional de *hackers* sobre tecnología y seguridad.

120 Toll Collect GmbH es una empresa que se encarga de gestionar el sistema de peaje a los camiones en las autopistas alemanas.

121 David John Cawdell Irving es un polémico escritor británico negacionista del holocausto judío.

122 Según las informaciones reveladas por WikiLeaks, en este ataque fallecieron al menos 91 civiles afganos y otros once resultaron gravemente heridos. El bombardeo de Kunduz, ordenado por el coronel alemán Georg Klein la noche del 3 al 4 de septiembre de 2009 —tras el robo y posterior abandono de dos camiones cisterna por parte de insurgentes—, provocó en Alemania una investigación parlamentaria sobre las responsabilidades en este asunto y un debate sobre la política de información del Gobierno germano. Este caso acabó con las dimisiones del jefe del Estado Mayor, Wolfgang Schneiderhahn, del secretario de Estado de Defensa, Peter Wichert, y del ministro de Trabajo, Franz-Josef Jung —que ocupaba la cartera de Defensa en el momento del ataque—, por haber ocultado el informe del incidente. La Fiscalía Federal cerró el sumario contra Klein al no encontrar indicios de violación del derecho internacional penal o del código penal alemán.

2010	5 de abril		WikiLeaks publica el vídeo *Collateral Murder*, que muestra el asesinato de doce civiles en Bagdad (Irak), ametrallados desde un helicóptero Apache del Ejército de Estados Unidos.
	26 de mayo		El soldado Bradley Manning es arrestado en Irak por filtrar documentos a WikiLeaks.
	Julio	Día 26	WikiLeaks publica los *Diarios de Guerra de Afganistán*, la primera filtración masiva de documentos secretos en colaboración con grandes medios de comunicación.
		Día 30	WikiLeaks añade en su página web un misterioso archivo encriptado con la etiqueta "Insurence" ("Seguro")[123].
	20 de agosto		WikiLeaks publica documentos sobre la planificación de la Love Parade celebrada en Duisburgo, Alemania[124].
			Se emite una orden judicial de captura en Suecia contra Julian Assange que poco después será retirada[125].
	26 de agosto		Julian Assange suspende a Daniel Domscheit-Berg temporalmente.
	Septiembre	Día 14	Domscheit-Berg repara un servidor de correo que funcionaba mal.
		Día 15	Domscheit-Berg y otros miembros abandonan WikiLeaks.
		Día 17	Se registra el nombre de dominio OpenLeaks.org.
	22 de octubre		WikiLeaks publica los *Diarios de Guerra de Irak*.
	28 de noviembre		WikiLeaks publica los cables diplomáticos de Estados Unidos.
	Diciembre	Día 1	Interpol emite una orden de captura internacional contra Julian Assange.
		Día 7	Assange se entrega a la Policía en Londres y es arrestado.
		Día 14	Assange es puesto en libertad bajo fianza.
		Día 30	Daniel presenta OpenLeaks.org en el Chaos Communication Congress (27C3).

Fuente: elaboración propia a partir de la cronología que aporta Daniel Domscheit-Berg en su libro *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website* (2011).

[123] A raíz de la condena del Gobierno de Estados Unidos por la liberación de miles de documentos de la guerra de Afganistán, WikiLeaks añadió en su página web de descargas de archivos sobre el conflicto afgano (http://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010) un misterioso archivo llamado *insurance.aes2560*, de 1,4 GB, encriptado con el algoritmo AES 256 (Advanced Encryption Standard es un esquema de encriptación avanzado por bloques adoptado como un estándar de cifrado por el Gobierno de los Estados Unidos). El *Insurance file* de WikiLeaks se ofreció también como *torrent* en páginas web de descargas como The Pirate Bay. Se especuló con que se trataría de una filtración cuya contraseña sería liberada en caso de que WikiLeaks sufriese algún ataque grave que hiciese que la organización quedase incapacitada. Tamién se dijo que sería una suerte de seguro de vida de Julian Assange.

[124] La Love Parade era un festival de música electrónica que se creó en 1989 en Berlín. La de 2010 fue su última edición, marcada por la tragedia al producirse una oleada de pánico en los túneles que culminaban el recorrido marcado por la organización, desde la estación central de la ciudad hasta una estación de mercancías abandonada, situada a unos 700 metros en línea recta. Dos recorridos delimitados de algo más de un kilómetro de longitud permitían a los asistentes ir de la estación central a la de mercancías, confluyendo ambos recorridos en el interior de un antiguo túnel para camiones de doscientos metros de longitud. Veintiuna personas fallecieron aquel trágico 24 de julio y hubo mas de trescientos heridos graves. La música continuó en el recinto a pesar de la tragedia, cesando a las 23 horas. Posteriormente, los organizadores anunciaron que no se volvería a organizar la Love Parade en señal de respeto a las familias de las víctimas.

[125] El 20 de agosto de 2010, una fiscal de guardia emitió la primera orden de captura contra Assange por un presunto delito de violación. La orden fue revocada 24 horas después por la fiscal jefe, que redujo el caso a un delito menor de acoso. El caso se reabrió cuando la fiscal superior, Marianne Ny, asumió posteriormente la dirección de la investigación por presunta violación, que culminó con una nueva orden de arresto contra Assange el 1 de septiembre de 2010.

IV.2. DESAFÍOS DE UN NUEVO MODELO DE ORGANIZACIÓN RED INFORMACIONAL Y TRANSNACIONAL EN EL HIPERESPACIO

IV.2.1. Organización apátrida

A finales de 2006, Julian Assange y un grupo de hackers y activistas pusieron en marcha "la primera «organización apátrida de información»", cuyo "objetivo, desde el principio, fue operar más allá del alcance de la justicia, conseguir documentos censurados por los gobiernos y corporaciones y hacerlos públicos" (Hastings, 2012: 46). Desde entonces, WikiLeaks se ha ido configurando como una organización red sin fronteras, nómada, desterritorializada, descentralizada e hiperespacial, exponente del hacktivismo informacional, que se confronta con la nueva ideología y paradigma del capitalismo y que funciona como un "mecanismo transnacional para difundir la información fuera del alcance de cualquier gobierno, empresa u organización" (Carr, 2011a). Uno de los grandes desafíos que plantea WikiLeaks es precisamente "la forma institucional de una organización internacional que actúa en el ciberespacio de una forma encaminada a frustrar la represalia y la regulación por medio de leyes nacionales de información" (Hood, 2011: 636)[126]. WikiLeaks se halla así en un limbo.

> El carácter itinerante y casi apátrida asumido por WikiLeaks —afirmado por Julian Assange como una salida límite para garantizar la seguridad de los colaboradores y la permanencia del sitio en la red— acaba por colocar el proyecto en un limbo legal y, a su vez, en un limbo organizacional o corporativo (Saad Corrêa, 2011: 217)[127].

En esta línea argumentativa, Sandra Braman aporta que "WikiLeaks, como una red autónoma, […] es un tipo de colectividad que aún no tiene estatus formal ante la ley" (Braman, 2014: 2605)[128]. Para esta autora, hay cinco tipos de sujeto de derecho implicados en las complejas cuestiones legales que plantea WikiLeaks, sobre los que aportamos ejemplos: 1) el individo —Julian Assange, Bradley Manning—; 2) la red WikiLeaks; 3) la red de redes asociadas que comparten objetivos con WikiLeaks y la apoyan —Anonymous, sitios web espejo, etc.—; 4) cualquier sujeto que haya hecho uso de información secreta proporcionada por WikiLeaks —fundamentalmente, periodistas y medios de comunicación que colaboran en las publicaciones de documentos secretos, pero también activistas, investigadores, etc.—, y 5) cualquier individuo que haya leído

126 Todas las citas tomadas de Hood (2011) son traducciones propias del texto original, en inglés.
127 Todas las citas tomadas de Saad Corrêa (2011) son traducciones propias del texto original, en portugués.
128 Todas las citas tomadas de Braman (2014) son traducciones propias del texto original, en inglés.

esos documentos y conocido los secretos de Estado y corporativos, accediendo a la base de datos de WikiLeaks en su sitio web o a las informaciones y cables publicados en medios de comunicación (Braman, 2014: 2606). Cinco sujetos de derecho sobre los que el peso del poder autoritario ha recaído de forma distinta: Manning, encarcelado y Assange, refugiado en la embajada de Ecuador en Londres para evitar su extradición; WikiLeaks, bloqueada económicamente; su red de redes colaborativas, acosada judicial y policialmente, y sus principales medios colaboradores, bajo la lupa y el control del Departamento de Defensa de Estados Unidos; sólo los ciudadanos receptores y sin implicaciones directas en las filtraciones —la masa— parecen librarse de la telaraña militar y judicial tejida sobre WikiLeaks, aunque intentan ser atrapados en otra telaraña propagandística.

IV.2.2. Nueva dimensión espacio-temporal

Los complejos problemas jurídicos que plantea WikiLeaks están intrínsecamente ligados a los cambios conceptuales, estructurales y funcionales que emergen de la realidad *trans* que todo lo atraviesa, que diluye los límites espacio-temporales, que sintetiza lo virtual y lo real, que reconfigura nuestra existencia y geografía sociopoítica, y que nos permite trascender también los límites del Estado-nación. Es en esta transrealidad hiperespacial donde WikiLeaks encuentra acomodo, como así lo evidencia Assange:

> Hubo un tiempo, en un lugar que no era ni aquí ni allá, en el que nosotros, los constructores y los ciudadanos de la joven Internet, discutíamos sobre el futuro de nuestro nuevo mundo. Vimos que las relaciones entre todas las personas serían mediadas por nuestro nuevo mundo y que la naturaleza de los Estados, definida por cómo la gente intercambia información, valores económicos y fuerza, también cambiaría.
>
> Vimos que la fusión entre las estructuras estatales existentes e Internet creaba la oportunidad de cambiar la naturaleza de los Estados. (Assange *et al.*, 2012: 2).

El desarrollo de la lógica red, arraigada en el informacionalismo, ha contribuido de manera decisiva a estas transformaciones en un nuevo mundo en el que las nociones del espacio y del tiempo han cambiado. La sustitución del espacio de los lugares y el tiempo histórico por el espacio de flujos y el tiempo atemporal, característicos de la sociedad red (Castells, 1997: 409-504; Himanen, 2001: 170-171),

permite a WikiLeaks manejarse en una nueva dimensión en la que, como ninguna otra organización, explota su potencial transformador.

> El tiempo y el espacio —que alguna vez se comportaron como barreras naturales, limitando el acceso a las instituciones, al igual que un foso— son ahora fáciles de superar. Quizás ninguna organización ha aprovechado de manera más prominente esta tendencia como WikiLeaks (Jurgenson y Rey, 2014: 2654)[129].

En Castells (1997), ahora el espacio organiza al tiempo en la sociedad red, que se construye sobre flujos de capital, información, tecnología, interrelaciones organizativas, imágenes, sonidos y símbolos. Estos flujos establecen un modelo espacial caracterizado por su dispersión y concentración simultáneas, y son la expresión de los procesos que dominan nuestra vida económica, política y simbólica. El soporte material de los procesos dominantes es el conjunto de elementos que sostienen esos flujos y hacen materialmente posible su articulación en un tiempo simultáneo (Castells, 1997: 445). Hay que considerar, además, que "el espacio de flujos no es indeterminado, sino que tiene una configuración *territorial* que está relacionada con los nodos de las redes de comunicación", esto es, su estructura y significado "no depende de ningún lugar en concreto sino de las relaciones construidas en el interior y alrededor de la red que procesa los flujos específicos de comunicación" (Castells *et al.*, 2007: 267).

La idea del espacio de flujos se encuentra en Assange, quien también prioriza el espacio como la dimensión que domina nuestra experiencia en red, en este caso mediada por Internet como espacio cognitivo. Para Assange, la Red es un "espacio de otro mundo", un "reino aparentemente platónico de flujo de ideas e información" que debería permitir un ágora global no intervenida, libre del las fuerzas coercitivas de los Estados-nación y de los actuales poderes fácticos autoritarios. Sin embargo, considera que la naturaleza platónica de la Red está "envilecida por sus orígenes físicos" (Assange *et al.*, 2012: 3), siendo realmente intervenida y determinada por el soporte material que configura los procesos dominantes del capitalismo global.

> Sus cimientos [los de la Red] son cables de fibra óptica que se extienden a través de los fondos oceánicos, satélites girando sobre nuestras cabezas, servidores informáticos ubicados en edificios en ciudades, desde Nueva York a Nairobi. Al igual que el soldado que mató a Arquímedes con una simple espada, una milicia armada también podría tomar el control del máximo desarrollo de la civilización occidental, nuestro reino platónico (Assange *et al.*, 2012: 3).

[129] Las citas tomadas de Jurgenson y Rey (2014) son traducciones propias del texto original, en inglés.

Assange nos introduce así en el problema central que aborda el hacktivismo informacional: el control *de facto* del espacio cognitivo, de los flujos de ideas e información por parte del poder autoritario, que implementa, mediante su dominio del espacio físico, mecanismos de control del espacio virtual.

> El nuevo mundo de Internet, abstraído del viejo mundo de átomos en bruto, anhelaba la independencia. Pero los Estados y sus amigos pasaron a controlar nuestro nuevo mundo mediante el control de sus puntales físicos. El Estado, como un ejército alrededor de un pozo de petróleo, o un agente de aduanas consiguiendo sobornos en la frontera, no tardaría en aprender a hacer uso de su control del espacio físico para conseguir el control de nuestro reino platónico. Éste impediría la independencia que habíamos soñado y, luego, ocupando líneas de fibra óptica y estaciones terrestres de comunicación por satélite, pasaría a interceptar masivamente el flujo de información de nuestro nuevo mundo, su esencia misma, a la vez que toda relación humana, económica y política se sumaba a él (Assange *et al.*, 2012: 3-4).

IV.2.3. Vigilancia global, control de la información y censura

En el capítulo III vimos cómo mediante mecanismos emocionales se estimulan rutinas de comportamiento en los internautas que favorecen el consentimiento e interiorización de la vigilancia global, conformando el panóptico perfecto que hace de cada nodo de la Red una torre de vigilancia Ahora bien, una infraestructura tecnológica robusta es necesaria para ejercer el control desde los centros de poder, canalizar sus resultados, almacenar masivamente los datos recolectados en el flujo de información y explotarlos política y económicamente. Así lo interpreta Assange:

> El Estado, como sanguijuela en las venas y arterias de nuestras nuevas sociedades, engulliría toda relación expresa o comunicada, cada página web leída, cada mensaje enviado y cada pensamiento *googleado*, para luego almacenar este conocimiento, miles de millones de interceptaciones al día, un poder inimaginable, en vastos almacenes secretos, para siempre. Luego pasaría a explotar una y otra vez este tesoro, la producción intelectual colectiva y privada de la humanidad, con algoritmos de búsqueda y detección de patrones cada vez más sofisticados, enriquececiendo el tesoro y maximizando el desequilibrio de poder entre interceptores e interceptados. Y entonces, el Estado plasmaría lo aprendido en el mundo físico: iniciar guerras, ataques con drones, manipular comités de la ONU y acuerdos comerciales, y hacer favores a su vasta red de industrias, infiltrados y compinches (Assange *et al.*, 2012: 3-4).

Más que nadie, hackers y hacktivistas son conscientes de que la Red sí es controlable y censurable, y de que la principal batalla se libra "sobre la infraestructura técnica de Internet y sobre los valores sociales que se pueden incrustar en esta infraestructura"; una batalla "sobre la naturaleza de los objetos tecnológicos y los

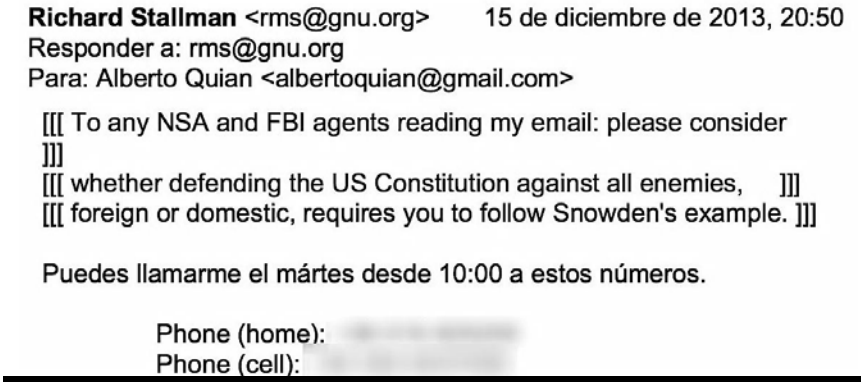
valores con los que estos objetos se crean" (Jordan y Taylor, 2004: 102). Por ello, los hacktivistas advierten:

> A medida que los Estados se funden con Internet y el futuro de nuestra civilización deviene en el futuro de Internet, debemos redefinir las relaciones de fuerza. Si no lo hacemos, la universalidad de Internet convertirá a la humanidad en una enorme red de vigilancia y control de masas (Assange *et al.*, 2012: 6).

Lejos de la proclamada Web *social*, para Stallman Internet está más próxima a convertirse en "un órgano de tiranía". El gurú de los hackers considera que las revelaciones de WikiLeaks y, sobre todo, de Edward Snowden, evidencian que "se han superado por mucho" los límites aceptables de control para una sociedad democrática, situándonos en un escenario pavoroso en el que "tenemos un nivel de vigilancia general mucho mayor que el que existía en la Unión Soviética" (Richard Stallman, en Quian, 2013c). Para los hackers, la amenaza es real, tanto, que Stallman acostumbra a encabezar sus correos electrónicos con un mensaje dirigido a la conciencia de los funcionarios del Gobierno de Estados Unidos, consciente de que cualquier comunicación puede ser interceptada por éstos:

> A cualquier agente de la NSA o del FBI que esté leyendo mi correo electrónico: por favor, considere si defender la Constitución de Estados Unidos de todos los enemigos, nacionales o extranjeros, requiere seguir el ejemplo de Snowden (Stallman, comunicación personal, 15 de diciembre de 2013).

Ilustración 18: Mensaje de Richad Stallman a los agentes de la NSA y del FBI.



Richard Stallman <rms@gnu.org> 15 de diciembre de 2013, 20:50
Responder a: rms@gnu.org
Para: Alberto Quian <albertoquian@gmail.com>

[[[To any NSA and FBI agents reading my email: please consider]]]
[[[whether defending the US Constitution against all enemies,]]]
[[[foreign or domestic, requires you to follow Snowden's example.]]]

Puedes llamarme el mártes desde 10:00 a estos números.

Phone (home):
Phone (cell):

Fuente: comunicación personal con Richard Stallman.

En esta contienda entre los ciberlibertarios y la autoridad, WikiLeaks se ha erigido en el catalizador de la preocupación central que moviliza a los hacktivistas: el libre flujo de información.

Lo cierto es que el Estado-nación aún se reserva mecanismos de control como los cortafuegos nacionales, construidos por algunos gobiernos para censurar contenidos, vigilar el acceso a Internet de los ciudadanos y asfixiar a los disidentes, como es el caso del Proyecto Escudo Dorado chino, por ejemplo. Uno de los objetivos principales del hacktivismo informacional ha sido cavar agujeros en esos cortafuegos para liberar en el ciberespacio a los ciudadanos cautivos dentro de las fronteras físicas de regímenes totalitarios que manipulan la infraestructura de Internet y controlan la información a escala nacional.

Métodos diferentes, pero fines similares, se manifiestan en el uso de sofisticados programas de vigilancia masiva a escala global por parte de la National Security Agency (NSA) de Estados Unidos. Sus poderosas herramientas tecnológicas permiten almacenar datos, metadatos, información, mensajes escritos, llamadas telefónicas, transacciones y movimientos, obtenidos de cables de fibra óptica y de servidores de grandes compañías tecnológicas —Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple, etc.—, además de vulnerar sistemas de encriptación y protocolos seguros financieros y comerciales, ejecutar ataques selectivos contra usuarios de la red TOR y usar técnicas de *cracking* contra instituciones, otras agencias de seguridad y operadores de telecomunicaciones.

Pero el control se extiende también desde los centros neurálgicos del poder corporativo. Richard Stallman, como otros muchos hackers, hacktivistas y *cypherpunks*, nos alerta de que el escenario *orwelliano*, el totalitarismo del Gran Hermano, ya está en marcha, y sus mecanismos son controlados conjuntamente por el imperio corporativo y el Estado-nación, capaces de invadir nuestra privacidad por puertas traseras, de vigilar nuestras comunicaciones, de recopilar nuestros datos, de cortar nuestras comunicaciones, de modificar o incluso borrar la historia, y de limitar nuestro acceso al conocimiento. Stallman ofrece un ejemplo ilustrativo de cómo el uso de tecnología controlada por grandes corporaciones empresariales compromete nuestra privacidad y libertad:

> ¿Sabe, por ejemplo, que Amazon borró remotamente miles de copias de un libro a los usuarios de Kindle? ¿Sabe qué libro? *1984*, de George Orwell. Esto simboliza el poder *orwelliano* que Amazon ejerce sobre los usuarios. Amazon es un produto *orwelliano* (Richard Stallman, en Quian, 2013c).

Stallman evoca un hecho que sucedió a mediados de julio de 2009, cuando Amazon invadió la privacidad de muchos usuarios de su lector de libros electrónicos Kindle para, sin previo aviso, borrar remotamente de sus dispositivos dos novelas de George Orwell: *1984* y *Animal Farm*[130]. Amazon alegó posteriormente que no tenía en regla los derechos de estas dos obras y decidió evitar problemas legales borrándolas de un plumazo. Obviamente, esto suscitó una gran polémica, ya que demostró hasta qué punto nuestra privacidad está comprometida y nuestro acceso al conocimiento, controlado por las grandes corporaciones tecnológicas.

Assange también observa un mecanismo de censura *orwelliano* en la desaparición selectiva de referencias *online* que son borradas de la Red para evaporar trozos de historia publicados alguna vez en un periódico, blog o red social en línea:

> La historia no sólo se modifica, sino que es como si nunca hubiera existido. Es la máxima de Orwell: «Quien controla el presente, controla el pasado y quien controla el pasado, controla el futuro.» Es la indetectable supresión de la historia en Occidente, y eso sólo tiene un nombre: censura postpublicación (Assange *et al.*, 2012: 121).

Todos estos ejemplos expuestos sobre el control que ejercen el imperio corporativo y el Estado-nación sobre el flujo de información, cuestionan la idea generalizada de que la estructura descentralizada de la Red y los reducidos costes de producción y distribución de la información configuran un sistema de inmunidad contra su control y censura (Jordan y Taylor, 2004: 100). La Red rechaza por su propia naturaleza la centralización del poder. Por su estructura rizomática, el control vertical, de arriba hacia abajo, es irrealizable, y el bloqueo de uno o varios nodos no impide que la información se siga distribuyendo por otros nodos interconectados. Sin embargo, se ha evidenciado que empresas y Estados-nación pueden poner barreras que bloqueen ciertos sitios de Internet para los usuarios que acceden a la Red, por ejemplo, desde los propios sistemas de estas empresas, que controlan el acceso de sus empleados, o desde equipos conectados en territorios hostiles a la libertad de información (Jordan y Taylor, 2004: 101). También se ha evidenciado la existencia de puertas traseras en el hardware y software que usamos masivamente; agujeros que nos hacen vulnerables.

130 Véase: 'Amazon Erases Orwell Books From Kindle', en http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html (último acceso: 12 de marzo de 2014).

IV.2.4. Nación y territorio desterritorizalizado

Sea a escala local, nacional o global, con cortafuegos o con programas intrusivos y de recolección de datos masivos, el control, la vigilancia y la censura en ciberespacio se ejerce, paradójicamente, sobre la base del territorio físico y se justifica, generalmente, en nombre de la seguridad nacional, evidenciándose la radical importancia que aún tiene el constructo de nación, el territorio como límite y la fortificación de sus fronteras, para mantener estructuras de poder autoritarias en una era de globalización del capital y cerco y aislamiento del individuo.

La conceptualización del ciberespacio no como dimensión comunicacional, sino como territorio de comunicación, como nuevo espacio fronterizo, es lo que permite las nociones de control y dominación en la dialéctica de la digitalización: "El espacio informacional de flujos se convierten en algo que las elites y las bases pueden intentar controlar como «de su propiedad»" (Jordan, 1999: 176). Pero el sentido de propiedad hacker, como hemos visto, difiere de la propiedad privativa inherente al capitalismo y de la propiedad territorial e identitaria del constructo nación. El hacker y todos los ciberlibertarios entienden que el ciberespacio les es propio, pero no exclusivo. Es un espacio abierto y compartido, un bien común, como el software libre, y ninguna fuerza ajena coercitiva ni privativa debería tener cabida en él. En esta retórica hacker subyace la idea de que los nacionalismos, todos, se curan viajando por el ciberespacio y con la ética hacker. Frente a la soberanía nacional, proponen la soberanía del individuo, con la que superar el territorio como parcela, la frontera como muralla, la identidad nacional como forma de segregación, la patria como privatización, el Estado-nación como poder coercitivo y fuente de conflictos.

Wray elucida que la naturaleza del ciberespacio es extraterritorial y, por lo tanto, quiere ser inmune a la autoridad del Estado-nación, que liga el cumplimiento de la ley a zonas geográficas delimitadas por jurisdicciones, sobre las cuales ejerce su potestad autoritaria; de manera que emergen "conflictos entre las nuevas capacidades de los agentes políticos y el viejo sistema del que la ley sigue dependiendo" (Wray, 1998), siendo WikiLeaks el ejemplo más clarificador de estas tensiones: cuando WikiLeaks libera la información secreta en el ciberespacio, esta se expande y se encuentra disponible a nivel global, trascendiendo los límites nacionales, circulando libremente de nodo en nodo.

Concebir el ciberesapacio como territorio parece, *a priori*, contradecir principios básicos de hackers y ciberlibertarios, que escapan de cualquier identidad nacional y de cualquier expresión identitaria definidas por los límites geográficos y simbólicos del Estado-nación y por su ordenamiento jurídico. Sin embargo, para los libertarios del ciberespacio el nuevo territorio fronterizo, en su forma pura, es un espacio abierto, habitado y configurado por individuos emancipados y libre de sesgos identitarios, religiosos, políticos, culturales o económicos. Un territorio sin más frontera que la que lo separa de los bordes geopolíticos, jurídicos, económicos y simbólicos que segregan a los individuos en el el mundo físico. Así lo explica Andy Müller-Maguhn:

> […] pienso que [los hackers] nos encontramos inmersos en una especie de conciencia común totalmente alejada de nuestras identidades nacionales —de ser alemanes, italianos, estadounidenses o de cualquier otro lugar—, sólo vemos que queremos resolver problemas, que queremos trabajar juntos. Vemos la censura de Internet, esta lucha de los gobiernos contra la nueva tecnología, como una especie de situación evolutiva que tenemos que superar (Assange *et al*., 2012: 156)

Es precisamente esa conciencia común la que configura un territorio desterritorializado, un ciberespacio desde el que "actuar sin problemas más allá de las fronteras geográficas y políticas, ya que estas fronteras no se manifiestan en el terreno" Wray (1998). En este territorio es donde WikiLeaks se protege y donde se configura como organización transnacional, apátrida y ubicua, que se sustrae a los controles geográficos, como así lo expone el propio Assange:

> […] tenemos esta sensación de que un ciberespacio —como una suerte de reino que, de hecho, existe en alguna parte—, lo es por su nivel de oblicuidad, complejidad y universalidad. Cuando lees algún archivo en Internet alojado en una ubicación es como si lo leyeras en cualquier otra, o en el futuro; ésa es su universalidad. De modo que en ese sentido, como organización que ocupa el ciberespacio, y como experta en mover su información a través de las incrustaciones subyacentes, tal vez seamos una organización postestatal, precisamente debido a esa falta de control geográfico (Assange *et al*., 2012: 127-128).

Desde el ciberespacio, WikiLeaks atraviesa y traspasa fronteras geográficas y simbólicas, y se proyecta hacia la vida física para materializarse en ésta y, desde ésta, reproyectarse en el ciberespacio, configurándose así en una organización hiperespacial que se vale de la criptografía para saltarse los controles fronterizos del Estado-nación. De nuevo, Assange dilucida:

> […] al resto de la prensa le gusta decir que somos una organización mediática sin Estado, y aciertan sobre la importancia de ser apátridas. […] si los activos de una organización son fundamentalmente su información, entonces puede ser transnacional de una manera difícilmente evitable gracias a la criptografía. Esto explica el bloqueo económico que se nos ha impuesto, pero otras facetas de nuestra organización son más difíciles de reprimir (2012: 128).

IV.2.5. Hiperespacio

La categorización de WikiLeaks como organización hiperespacial responde a la necesidad de tomar un concepto holístico como categoría de análisis; un concepto que nos permita explicar el espacio de flujos que brota de la fricción entre el espacio físico y el espacio cíber. Ya en Gómez Cruz (2002, 2003) aparece el concepto de hiperespacio para intentar comprender y analizar cómo operan ambos espacios combinados. Su propuesta nace de las interpretaciones de Mitra y Schartz (2001) de los espacios cibernéticos como síntesis de lo real y lo virtual. Para Gómez Cruz, la domesticación de las tecnologías que dan acceso al ciberespacio y la virtualización del hogar, sirven para justificar la proposición del hiperespacio como constructo para explicar "la relación que establecen los sujetos con los objetos tecnológicos y los espacios simbólicos que la comunicación mediante éstos genera" y, sobre todo, "el impacto que tiene esta conjunción de espacios en el sujeto" (2003: 31).

En el hacktivismo, en general, y en WikiLeaks, en particular, se evidencia esta dimensión hiperespacial en la que convergen el espacio físico y el espacio cíber y en la que se reconfiguran el uno al otro.

IV.2.6. Transnacionalización capitalista y transnacionalidad libertaria

Es necesario ahora explicar brevemente la diferencia que existe entre la transnacionalización capitalista como mecanismo de colonización y homogeneización de espacios económicos, y la idea de transnacionalidad aplicada al individuo ciberespacial como vía de liberación. La idea de la transnacionalización se ha aplicado casi exclusivamente con criterios economicistas desde que el capitalismo neoliberal convirtió las redes de producción transnacionales en paradigma y motor del proceso de globalización, o más precisamente, del proceso que favorece la hegemonía de elites económicas ahora a escala global. Sin embargo, desde otra perspectiva sociológica

centrada en los efectos que el uso de las redes de comunicación electrónicas tienen en la configuración de nuevas relaciones sociales, se observa que la dimensión global de la Red facilita el ideal ciberlibertario del individuo libre que trasciende los límites del Estado-nación y combate las redes transnacionales capitalistas fortaleciendo alianzas y coaliciones en redes activistas, también transnacionales, impregnadas del "carácter irreverente, igualitario y libertario de la cibercultura" (Norris 2001: 191).

WikiLeaks se ha protegido, pero también fortalecido precisamente en su configuración como red de redes transnacional: redes informativas, redes activistas y hacktivistas, redes políticas, redes de espejos web, redes de donaciones, redes sociales, se articulan en el interior y alrededor de la red WikiLeaks, sin fronteras que las frenen. Redes tejidas en el espacio cíber y en el espacio físico por nodos autónomos que, interconectados, conforman una híper-red global. Y esto es lo que hace inabordable e impenetrable el fenómeno WikiLeaks para el poder autoritario. Cuando un nodo de la red WikiLeaks es desconectado o interrumpido, otros nodos son activados o reactivados.

IV.3. HACKTIVISMO INFORMACIONAL

Con la aparición de WikiLeaks a finales de 2006, surge un nueva estrategia informacional amplificada, híbrida, transversal, transnacional y en red que prioriza tácticas troyanas para introducirse y subvertir el sistema por tres vías: las redes secretas de información, las redes públicas de información y la política institucional. En lugar de alterar, colapsar, bloquear o dañar las corrientes informativas del poder autoritario, al estilo del hacktvismo más radical y reactivo, el hacktivismo informacional busca penetrar sutilmente en éstas para acceder al flujo de información secreta, hacerla pública y manejarla estratégicamente. En este nuevo enfoque hacktivista, también el código informático deja de ser la única herramienta para esquivar la censura, proteger la identidad y las comunicaciones de los disidentes, o colarse en el sistema nervioso del poder institucional. Si antes el código computacional era la llave hacker para infiltrarse en los sistemas informáticos de gobiernos y corporaciones empresariales, o la herramienta para sortear cortafuegos, ahora se recurre también a un código emocional que interviene en la conciencia de los sujetos que sirven desde dentro al poder gubernamental y corporativo, para que lo subviertan y liberen información secreta de interés público. Un ejemplo de esto es el mensaje que hemos visto en los correos electrónicos de Richard Stallman, en los que apela a la conciencia de los funcionarios del FBI y de la NSA que rastrean comunicaciones para que sigan el ejemplo de Edward Snowden, el exempleado de la National Security Agency que decidió revelar los programas de vigilancia masiva y global del Gobierno estadounidense, impactado también por un código emocional, en este caso el *escrito* por WikiLeaks y Bradley Manning. Este código *sensitivo* también opera activando políticamente a multitudes de individuos en el ciberespacio y en las calles. Es emocional porque afecta a la *sensibilidad* humana —a los sentidos y a los sentimientos— y contagia la emoción de la disidencia.

Con el hacktivismo digitalmente correcto definido por Jordan y Taylor (2004), el código informático adquirió un valor que no es intrusivo, sino defensivo, como instrumento para la protección de los disidentes, cuyas comunicaciones son encriptadas y sus identidades, protegidas. Pero ahora el código informático funciona, además, como elemento persuasivo para potenciales confidentes que se hallan en el mismo sistema nervioso del poder: la encriptación se publicita como garante de la seguridad que

necesitan los confidentes para filtrar los secretos de Estado o corporativos que manejan. La información filtrada por éstos es gestionada por expertos en tecnología, activismo y comunicación e información, que deciden *cómo*, *cuándo* y *dónde* se mostrará.

El *cómo* implica a la vez atención a la ética que debe regir la gestión de esa información y a las distintas maneras en las que la información obtenida debe ser expresada; el *cuándo* decide el momento oportuno en el que la información debe ser liberada, y el *dónde* comprende todos los espacios, físicos y cíber, donde volcar esa información para su uso público: medios de comunicación tradicionales y alternativos, canales de información propios, conferencias, charlas o foros, pero también en los propios parlamentos, en las cámaras de representación donde se legisla y se ejecuta el poder político. La creación del WikiLeaks Party en Australia y la irrupción en Europa del Partido Pirata en parlamentos nacionales y en la Eurocámara, además de la búsqueda y difusión de apoyos entre representantes políticos de todo el mundo, evidencian este interés del hacktivismo informacional por penetrar en los órganos de decisión del Estado también por la vía institucional.

El *cómo* se ha revelado dilema al suscitar tres controvertidos debates: 1) sobre el secreto de Estado y los riesgos de la publicación de información y datos confidenciales para la seguridad nacional *vs* los beneficios de la transparencia para la democracia; 2) sobre la protección de las fuentes del gobierno *vs* la seguridad de las fuentes de los hacktivistas; 3) el debate periodístico sobre el uso mercantil que los medios de comunicación convencionales hacen de la información *vs* el papel de medios alternativos como contrapoder.

El *cuándo* se ha convertido en un factor estratégico clave para gestionar la tensión informativa y maximizar el impacto del mensaje hacktivista.

El *dónde* se ha expandido para alcanzar todas las esferas en las que se produce y gestiona la opinión pública.

Esta nueva forma de hacktivismo, ahora complejamente estructurado, inspira y orienta otras manifestaciones activistas y hacktivistas en los espacios físico y virtual, a la vez que se ofrece como auspicio, soporte o asistente de éstas y de aquellos individuos que subvierten el Estado de secreto (confidentes, disidentes, activistas y periodistas comprometidos con la libertad de información y la transparencia).

El hacktivismo del siglo XXI, de la mano de WikiLeaks, pero también de Anonymous, ha dejado de ser exclusivamente la expresión política de técnicas de *hacking* informático; ahora no sólo recurre a la máquina, también apela al ser humano, a la *sensibilidad* del individuo y a la filosofía de nuestro tiempo.

El enfoque transversal del hacktivismo informacional lo lleva a balancearse entre el terreno institucional (en los medios convencionales y en los registros oficiales de marcas, organizaciones y partidos políticos) y el de la clandestinidad (protección de identidades y de ubicaciones). Y lo impulsa a abrirse a una nueva dimensión económica compleja, necesaria para mantener la infraestructura técnica y los recursos humanos, ejecutar proyectos, proteger las fuentes, defenderse legalmente y ser competitivo en un ecosistema informacional dominado por las grandes corporaciones mediáticas y las transnacionales tecnológicas.

¿Qué significa esta nueva arquitectura informacional para el hacktivismo? Moglen (1999) considera que el concepto mismo de desarrollo social se está alejando de la posesión de industria pesada, basada en motores de combustión interna, hacia una postindustria basada en comunicaciones digitales y formas de actividad económica basadas en el conocimiento. Es lo que Castells (1997) llama sociedad informacional, dominada por el capitalismo cognitivo. Para Castells, los dos elementos importantes de cualquier economía —la productividad y la competitividad— dependen ahora fundamentalmente de la capacidad de adquirir conocimiento y de procesar información. En concreto, explica:

> […] el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la trasmisión de información se convierten en una de las fuentes fundamentales de la productividad y el poder debido a las nuevas condiciones que surgen en este período histórico (Castells, 1997: 47).

Castells aclara que lo que caracteriza al informacionalismo no es el papel central del conocimiento y la información en la generación de riqueza, poder y significado, ya que el conocimiento y la información siempre han estado estrechamente asociados a la dominación político y militar, la prosperidad económica y la hegemonía cultural. Por lo tanto, en cierto sentido, todas las economías se basan en el conocimiento, y todas las sociedades son sociedades de la información. Para Castells, lo distintivo de nuestra

época es el nuevo paradigma tecnológico marcado por la revolución en las tecnologías de la información y la comunicación, que ha aumentado la capacidad humana de procesamiento de información y de generación y aplicación del conocimiento (2001: 158-159).

WikiLeaks se ha adaptado como ninguna otra organización hacktivista a este paradigma, al entender que para ser una organización competitiva debía asumir costes y riesgos tangibles e intangibles para aumentar y optimizar su capacidad de producir información y de generar conocimiento, y ampliar su impacto e influencia, articulando una estructura en red que lo atravesase *todo* y ampliando su capacidad *parasitaria* en el mismo núcleo de los poderes político-corporativo y mediático, donde se genera, se procesa y se transmite la información realmente potente. Esto obliga a la organización a diseñar un modelo económico sostenible que le permita mantenerse competitiva. Se configura así un nuevo modelo de organización informativa, basada en principios hackers y que, a diferencia de la empresa informativa clásica, se declara sin ánimo de lucro y rehúye de la publicidad y de cualquier mecanismo económico de control editorial, asegurando la viabilidad de su libertad y su funcionamiento como verdadero servicio público —transparente, abierto, accesible a cualquier individuo en cualquier momento y desde cualquier lugar— mediante donaciones y venta de *merchandising*. WikiLeaks explota así una dimensión económica nueva basada en la cooperación, que se opone a la clásica dimensión económica capitalista. A la cosificación de la información y su gestión como mera mercancía se responde con la *humanización* de la información como fuente de conocimiento y su gestión altruista. Cada céntimo recibido por donaciones o venta de *merchandising* es por y para la información; cada camiseta, sudadera, bolso, mochila, taza o póster vendido con el sello de WikiLeaks denota, además, un acto de adhesión y de cooperación para expandirlo del ciberespacio al espacio físico.

IV.4. JULIAN ASSSANGE

IV.4.1. Un fenómeno narratológico

La figura de Julian Assange, como paradigma del nuevo disidente intelectual en los tiempos virales, ha originado toda una variedad de relatos y especulaciones en los medios de comunicación. Para sus colaboradores y seguidores, "Assange es un valiente defensor de la verdad"; sin embargo, para sus enemigos y detractores sólo es alguien que "busca autopromoción, poniendo en peligro vidas al hacer pública una gran cantidad de información sensible", dice una reseña de la cadena pública británica BBC[131].

"¿Es WikiLeaks el sueño de un idealista, o una herramienta para manipular la política mundial? ¿Quién es realmente Julian Assange? Dice que su sueño es un mundo sin secretos. Pero, ¿es eso cierto?", se pregunta por su parte el canal de noticias ruso RT en un amplio reportaje audiovisual titulado *The man who leaked the world*[132], un intencionado símil con *The man who sold the world*, la celebérrima canción del artista británico David Bowie de su disco homónimo, publicado en 1970, en la que *El Duque Blanco* exploró los moldes de identidad, los personajes ficticios en los que nos escondemos para conquistar el mundo, y que están en permanente fricción con la genuina personalidad desertada, que deviene en anhelo cuando aflora la inexorable crisis de identidad del individuo que fabula su *yo* en el permanente conflicto entre su *ello* y su *superyó*.

El hombre que filtró el mundo, sacando a la luz los secretos inconfesables del Estado-nación, es el mismo al que la edición italiana *Rolling Stone* declaró *rock star* de 2010 y le dedicó en exclusiva la portada de su número de diciembre de 2010, en la que aparece Assange sentado frente a varios televisores, simulando la icónica imagen de David Bowie en la película de Nicolas Roeg *The Man Who Fell to Earth* (1976), en la que el artista londinense interpretó a un alienígena humanoide. Pero esta vez, el *alienígena humanoide* viene de un mundo llamado Red: *The Man Who Fell (From the Web) to Earth*.

131 Disponible en: http://www.bbc.com/news/world-11047811 (último acceso: 6 de diciembre de 2012).
132 Disponible en: https://www.rt.com/shows/documentary/assange-leaked-world-manipulate/ (último acceso: 6 de diciembre de 2012).

Ilustración 19: Portada de la edición italiana de *Rolling Stone* dedicada a Julian Assange (diciembre de 2010) e imagen de David Bowie en el filme *The Man Who Fell to Earth* (1976).

Fuente: http://noticias.lainformacion.com/arte-cultura-y-espectaculos/julian-assange-emula-a-david-bowie-en-la-portada-italiana-de-rolling-stone_Dgd70P8u2F81UOt4NmKp8/ (último acceso: 8 de diciembre de 2012).

Pero, ¿quién es realmente Julian Assange? ¿El idealista anarquista de la información que florece de creencias populares, héroe y libertador de las masas subyugadas por el omnipotente Estado-nación? ¿El icono *pop* hipermoderno que vende la industria del espectáculo? ¿El ciberterrorista y agresor sexual de la versión del Estado-nación? ¿Es Assange quien dice ser? ¿Es quien decimos, o es quien nos dicen?

Julian Assange —personificación de la libertad o del ciberterrorismo, según convenga— es un fenómeno narratológico idiosincrásico de esta era de redes, paradigma de la convergencia mediática, la cultura participativa y la inteligencia colectiva (Jenkins, 2008), en la era de la transrealidad. Julian Assange es una historia de historias ubicua y multicrónica en una realidad líquida que altera el vínculo lineal entre pasado, presente y futuro; realidad que expande en el hiperespacio intemporal en el que se conectan el ciberespacio y el espacio físico, y donde se desarrollan los múltiples relatos, sin principio ni fin, del héroe mitológico y del villano herético, encarnados en un mismo ser ambiguo, dilatado, sugestivo y evocador, con un agitado y accidentado pasado, un intrincado presente y un futuro bífido que se enredan en el universo-red.

La historia de Wikileaks es la historia de Julian Assange. Y Assange es, en definitiva, el protagonista de la primera gran *wikistory* de nuestra era. Una historia colaborativa, de múltiples voces y versiones en múltiples medios, soportes y plataformas, que trasciende al hombre. Como bien arguyen los periodistas de *The*

Guardian que colaboraron en las filtraciones masivas del año 2010, "resulta imposible contar esta historia sin contar la historia del propio Julian Assange, aunque está claro que el tema global de WikiLeaks y la filosofía que representa tienen un significado mucho más duradero" (Leigh y Harding, 2011: 20).

La de Julian Assange es una historia de historias desarrollada por los *storytellers* de la política y de los medios de información, pero también por los grupos de apoyo a WikiLeaks y, principalmente, por el propio Assange. El *storytelling* es una técnica de comunicación, control y poder para "imponer ideas, generar sentido y controlar las conductas", pudiendo convertirse en una poderosa "arma de distracción masiva" que "no admite el estatus de ficción" (Salmon, 2008: 12-13). Esto explica que versiones sobre Assange contradictorias, antagónicas e impregnadas de elementos fabulosos, sean aprehendidas como realidad y verdad, en forma de relatos de tintes novelescos y cinematográficos propios del *thriller* de seguridad nacional.

> La cooperación Hollywood-Pentágono —escribía Maurice Ronai[133]— ha hecho posible la emergencia de un nuevo género: el *thriller* de seguridad nacional, que tiene por resorte narrativo la puesta en escena de «desafíos asimétricos» […] La inventiva de los guionistas en las descripciones de las «amenazas» y de las «crisis» se completa con una gran desenvoltura en la representación del enemigo: mafia, grupo terrorista, *rogue state* (Salmon, 2008: 181-182).

Convertido en un fenómeno narratológico transmediático y viralizado en Internet a través de múltiples canales, Assange adquiere el estatus de mito policonstruido, que encuentra perfecto acomodo en tiempos de globalización de inseguridades, incertidumbres, inestabilidades y convulsiones políticas, económicas y sociales, como los que vivimos en los albores del siglo XXI: desde el nuevo orden mundial establecido tras los atentados del 11 de septiembre de 2001 en Estados Unidos, hasta la crisis económica global y los recortes del Estado de Derecho en las economías capitalistas de Occidente:

> La resurgencia de los mitos en el seno de nuestra sociedad contemporánea, afirmaba [Georges] Lewi[134], se confirma más particularmente en periodos de inseguridad mundializada que estimulan nuestra necesidad de búsqueda de verdad, de sentido de la vida, así como nuestra sed de magia y de misterio (Salmon, 2008: 62).

[133] Maurice Ronai es un político socialista francés, experto en comunicación política y tecnologías de la información, autor de varios documentales y miembro de la Commission Nationale de l'Informatique et dês Libertés de Francia.

[134] Georges Lewi es director general del Instituto BEC (Branding Experts Center) de París, profesor en la Sorbona y en la Escuela de Estudios Superiores de Comercio de París.

Narrar, simular, persuadir y movilizar, fundamentalmente tocando las emociones. He aquí las claves de esta primera gran *wikistory* en la sociedad red: la vida y obra de Julian Assange.

IV.4.2. Orígenes ideológicos: cultura hacker y *cypherpunk*

IV.4.2.1. Mendax, el hacker

Nacido el 3 de julio de 1971 en Townsville, en el estado australiano de Queensland, Julian Assange tuvo una infancia y una juventud agitadas, de tintes novelescos. Assange creció en el seno de una familia nómada y huidiza que responde al perfil acordado socialmente de familia desestructurada. La familia de Assange estaba vinculada al mundo del teatro de marionetas y era perseguida por una secta religiosa a la que pertenecía Keith Hamilton, padre de un medio hermano del fundador de WikiLeaks. Assange pasó por treinta y siete colegios diferentes y seis universidades.

Con 14 años de edad tuvo sus primeros contactos con la informática por medio de una computadora Commodore 64; a los 17 ya estaba *hackeando*; con 18 años se casó y fue padre de un niño, Daniel, al que perdió de vista veinte meses después, cuando su esposa huyó por la presión policial que estaba sufriendo el grupo de hackers con el que se movía siempre Assange en Melbourne. En 1991 ya era un avezado y reputado hacker, y fundó junto con otros dos colegas, conocidos como Prime Suspect y Trax, la revista *International Subversive*; ese año fue detenido por primera vez, por la unidad de delitos informáticos de la Policía Federal australiana, por haber entrado ilegalmente en la terminal central de la empresa de telecomunicaciones canadiense Nortel, la sede del 7º Grupo de Mando de las Fuerzas Aéreas estadounidenses en el Pentágono, el Naval Surface War Center de Virginia, la planta de Sistemas Técnicos Aeroespaciales de Lockheed Martin en California y MILNET, la red de datos secretos del Ejército de Estados Unidos, entre otras hazañas informáticas (Leigh y Harding, 2011). Assange no fue acusado hasta el año 1994. Se le atribuyeron veinticuatro delitos, por los que fue juzgado en 1996 en el Tribunal de Justicia de Victoria County de Melbourne, y salió en libertad tras pagar una multa de 2.100 dólares.

Por entonces, Assange ya estaba participando activamente en la lista internacional de correo electrónico *Cypherpunks*, donde se nutrió de las ideas de los

ciberlibertarios más radicales desde principios de 1994 hasta el verano de 2002, cuando la abandonó (Manne, 2011).

Durante la primera mitad de los años noventa, Assange adquirió un estatus simbólico como el hacker más famoso de Australia, bajo su pseudónimo Mendax[135], el mismo personaje que aparece en el libro *Underground*, escrito por Assange junto con la periodista Suelette Dreyfus a mediados de la pasada década de los noventa. La publicación en 1997 de este libro de investigación, con evidentes tintes autobiográficos y escrito al más puro estilo de una docunovela sobre los primeros disidentes informáticos de la década de los ochenta y primeros años noventa, marca el culmen de la primera parte en la que se puede dividir la biografía de Assange, quien empezaría a escribir una nueva historia personal, el segundo episodio de su novelesca vida, con la gestación y puesta en marcha de WikiLeaks en 2006. Es a partir de entonces cuando su historia ha adquirido verdaderos tintes de *thriller*.

IV.4.2.2. Editor hacker

Desde que Assange decidió salir del anonimato en el que se protegía como principal responsable del proyecto WikiLeaks, ha intentado desvincularse de la etiqueta *hacker* (Greenberg, 2010). Sin embargo, su formación como tal, su naturaleza *cypherpunk*, su actividad mediada por las computadoras y su participación activa en el movimiento del software libre no se lo posibilitan. Nadie ilustrado le niega al fundador de WikiLeaks su naturaleza hacker. Levy reconoce en Assange una mentalidad propia de esta cultura y Richard Thieme ve en WikiLeaks un fruto de la ética hacker (Knappenberger, 2012).

El interés de Julian Assange en que no se le identifique con aquéllos con los que comparte una ética —Assange mantuvo como hacker una enardecida defensa de célebres colegas encarcelados en Estados Unidos, como Mitnick o Cummings (Manne, 2011)— forma parte de su estrategia para conseguir la confianza de los ciudadanos y ganar credibilidad ante una opinión pública *infotoxicada* en temática hacker, a la vez

[135] Mendax es un pseudónimo inspirado en un verso de las *Odas* de Horacio, la undécima del III libro, en el que se dice, en latín, "splendide mendax" ("espléndido engaño"). Mendax es el "gran mentiroso". Como explican los periodistas de *The Guardian* David Leigh y Luke Harding en su libro *WikiLeaks y Assange. Un relato trepidente sobre cómo se fraguó la mayor filtración de la historia* (2011), la madre de Assange lo había introducido con entusiasmo en los clásicos grecolatinos. Como iremos viendo en este trabajo, las referencias a la mitología griega están muy presentes en la vida del fundador de WikiLeaks.

que intenta obtener legitimidad y ciertas protecciones legales para él y su organización. Por eso, el fundador de WikiLeaks prefiere presentarse como periodista y editor de una publicación —posición que le reservaría derechos fundamentales protegidos, como la libertad de expresión y de información, o la protección de sus fuentes, entre otros—, y no como miembro de una comunidad criminalizada por el poder político y los medios, y penalizada socialmente.

Assange entiende que hay una razón muy específica para que se le presente sólo como hacker:

> Hay un intento deliberado de redefinir lo que estamos haciendo no como una publicación, lo cual está protegido en muchos países, o como actividades periodísticas, lo cual tiene distintas protecciones, sino como algo que no tiene protección, como el *hacking*, y por lo tanto buscan separarnos del resto de la prensa y de estas protecciones legales. Es un intento deliberado de algunos de nuestros oponentes. Y se hace también por el miedo que medios como *The New York Times* tienen a ser regulados e investigados si incluyen nuestras actividades en la edición y el periodismo (Assange, en Greenberg, 2010).

Este temor a ser identificado como hacker —en el significado peyorativo que le atribuyen los medios tradicionales— ha sido una de las principales preocupaciones de Assange en su intento por ganar para WikiLeaks el apoyo de potenciales filántropos y colaboradores, y la simpatía de la población en general: "[Assange] sabía que si WikiLeaks quería prosperar, y también ganarse el apoyo de organismos filantrópicos como la Fundación Soros, el origen hacker-criptopunk del núcleo [de WikiLeaks] necesitaba ser disfrazado" (Manne, 2011)[136]. Esto se evidencia en un correo que Assange envió a John Young el 26 de diciembre de 2006. En éste, Assange se muestra consciente de la necesidad de que, en sus orígenes, WikiLeaks se mostrase como una organización liberal moderada (Manne, 2011) que trabaja por los derechos humanos, la democracia, el buen gobierno y la libertad de prensa, y no como carnaza para otro manido titular del estilo "hackers atacan de nuevo" (WikiLeaks Leak, 2007).

Esto es lo que justifica que Assange se desprenda de su esencia hacker en una teatralidad que abandona cuando, lejos de miradas furtivas, se aísla para escribir código en una computadora y *hackear* el mundo. Sin embargo, en el fundador de WikiLeaks reconocemos a la vez a un hacktivista y a un editor (Manne, 2011).

[136] Las citas tomadas de Manne (2011) son traducciones propias del texto original, en inglés.

IV.4.2.3. *Cypherpunk*: principios filosóficos

Para entender mejor a Julian Assange y WikiLeaks, y comprender sus motivaciones, objetivos y estatregias, es necesario adentrarse en el movimiento *cypherpunk*, donde se hallan las raíces políticas y filosóficas del fundador de WikiLeaks (Manne, 2011).

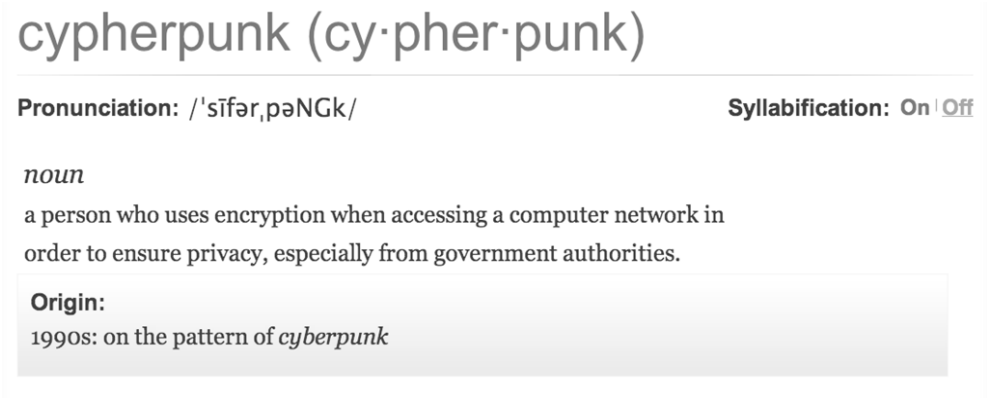
El *cypherpunk* es una evolución del *cyberpunk* para describir a los seguidores de este subgénero de ciencia ficción con ideales libertarios y que utilizan la criptografía computacional para proteger sus comunicaciones. El *cyberpunk* nació a finales de la década de 1970 como yuxtaposición entre la actitud punk y la alta tecnología: toma su nombre de la combinación entre cibernética y punk. La cibernética es una ciencia interdisciplinaria cuyo nacimiento se fija en la década de 1940. Se encarga del estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas, y de cómo aplicar mecanismos de regulación biológica a la tecnología. El punk, por su parte, fue un movimiento musical y contracultural surgido a mediados de la década de 1970, participado por *outsiders* que transgredieron las normas éticas y estéticas para liberarse de lo que consideraban estigmas sociales. Los punks cultivaron el nihilismo, el anarquismo, el escepticismo, la ética *do it yourself* y el libre albedrío; cuestionaron las convenciones sociales y la cultura de masas, e hicieron popular el lema *"No future"*, axioma distópico del posmodernismo. Ese distopismo es el que adopta el *cyberpunk*, como subgénero de ciencia ficción, a finales de esa década y en los años ochenta del siglo XX, para recrear un futuro próximo oscuro, siniestro, determinado y dominado por la alta tecnología, en el que el ser humano no es más que una rata de laboratorio en manos de grandes corporaciones empresariales transnacionales que han sustituido a los Estados-nación.

El término *cypherpunk* fue acuñado por Jude Milhon[137] como un juego de palabras entre *cypher* (código cifrado) y *cyberpunk* (punk cibernético), para denominar a un pequeño grupo de ciberlibertarios creado por Eric Hughes, Timothy C. May y John Gilmore en septiembre de 1992, que se reunían mensualmente en la compañía de

[137] Más conocida en los círculos informáticos y del hacktivismo como St. Jude, Milhon (1939-2003) fue una programadora informática, hacker, escritora, editora de la revista *Mondo 2000*, defensora de los ciberderechos y de la participación activa y decisiva de las mujeres en la Red, y uno de los primeros miembros del movimiento *cypherpunk*. Tras su muerte, Michelle Delio le dedicó un artículo publicado en la revista *Wired*, el 22 de julio de 2003, que tituló *Hackers Lose a Patron Saint* (*Los hackers pierden una Santa Patrona*). Disponible en: http://archive.wired.com/science/discoveries/news/2003/07/59711 (último acceso: 12 de enero de 2013).

Gilmore, Cygnus Solutions, en San Francisco. Los tres padres fundadores del *cypherpunk* pusieron en marcha la lista de correo electrónico *Cypherpunks* para hablar y debatir sobre criptografía y sus efectos en la sociedad. Se estima que en el año 1997, cuando esta lista de correo electrónico alcanzó su cenit, unas dos mil personas estaban participando en la "cruzada político-ideológica" *cypherpunk* (Manne, 2011).

La palabra *cypherpunk* fue incluida en septiembre de 2006 en el Oxford English Dictionary[138], que define así este neologismo: "Una persona que usa la encriptación cuando accede a una red informática para proteger su privacidad, especialmente de la autoridad gubernamental"[139].


cypherpunk (cy·pher·punk)

Pronunciation: /ˈsīfərˌpəNGk/ **Syllabification:** On | Off

noun

a person who uses encryption when accessing a computer network in order to ensure privacy, especially from government authorities.

Origin:

1990s: on the pattern of *cyberpunk*

El diccionario hacker Jargón File ofrece una definición similar para la palabra *cypherpunk*, que se usa para denominar a "alguien interesado en el uso de la criptografía a través de sistemas de cifrado electrónicos, para mejorar la privacidad personal y la protección contra la tiranía de estructuras de poder centralizadas y autoritarias, especialmente de gobierno" (The on-line hacker Jargon File, version 4.4.7, 29 de diciembre de 2003).

El *cypherpunk* hereda los principios hackers que animan a desarrollar y mantener una "hostilidad instintiva contra la censura, el secreto, el uso de la fuerza o el engaño" que se ejerce desde el poder institucionalizado, de manera que el sistema de poder coercitivo debe ser hackeado, pues "los autoritarios prosperan en la censura y el secreto, y desconfían de la cooperación voluntaria y el intercambio de información; sólo

[138] Lista de nuevas palabras incluidas el 14 de septiembre de 2006 en el Oxford English Dictionary: http://www.oed.com/public/update0609/september-2006-update (último acceso: 13 de enero de 2013).
[139] Véase en: http://www.oxforddictionaries.com/es/definicion/ingles/cypherpunk (último acceso: 13 de enero de 2013).

les gusta la «cooperación» que controlan" (Raymond, 2001). Sin embargo, el objetivo *cypherpunk* de desmantelar el Estado de secreto no debe entrar en conflicto con el derecho a la privacidad de cada individuo, como se asume en el *Manifiesto Cypherpunk*, firmado por Eric Hughes el 9 de marzo de 1991:

> La privacidad es necesaria para una sociedad abierta en la era electrónica. Privacidad no es secreto. Un asunto privado es algo que no queremos que todo el mundo sepa, pero un asunto secreto es algo que alguien no quiere que nadie sepa. Privacidad es el poder de revelarse uno mismo al mundo de forma selectiva (Hughes, 1991).

O dicho con otras palabras, las del hacker Richard Stallman:

> La lucha es entre el secreto del Estado y la democracia. Los ciudadanos no podemos tener el control del Estado sin saber qué hace éste. Y para la democracia también hace falta el derecho a la privacidad del individuo (Richard Stallman, en Quian, 2013c).

El objetivo último del movimiento *cypherpunk* es proteger, mediante la encriptación, la privacidad del individuo en sus actividades comerciales y relaciones sociales mediadas por las tecnologías, asegurando que la información circule libremente por túneles de la Red seguros, de modo que se garantice así un verdadero mercado libre y una vida plenamente soberana, fuera del alcance de gobiernos y corporaciones que buscan mantener su hegemonía mediante su control sobre los flujos de información y los procesos productivos, comerciales y sociales. La privacidad del individuo desafía, por lo tanto, el imperio corporativo-gubernamental, debilitando la eficacia de sus mecanismos de control, sustentados principalmente en el secreto, la vigilancia y la censura.

Los *cypherpunks* entienden que el Estado de secreto tiene que ser desmantelado como parte del proceso hacia la consecución de una sociedad ideal. Müller-Maguhn arguye que el objetivo del secreto es limitar la cantidad de personas que conocen un proceso y, por lo tanto, la capacidad de afectar al proceso mismo (Assange *et al.*, 2012: 22-23). Julian Assange, por su parte, identifica el secreto como una herramienta de censura y ve en la búsqueda y liberación de información oculta el camino hacia un estado global de verdadero conocimiento y de auténtica justicia. En el documental *WikiLeaks: Secretes and Lies*, el fundador de WikiLeaks expone de manera sucinta:

> Todos los organismos, todos, están metidos en actividades injustas. Así que cuando intentas encontrar la información que puede dar lugar a un estado de justicia mejorada, buscas la que el organismo no quiere que se conozca. Siempre he dicho que la censura, aunque sea algo condenable, siempre es una señal optimista, siempre es una oportunidad, porque la censura revela el miedo a la reforma por medio del conocimiento (Assange, en Forbes, 2011)[140].

El ideal de la emancipación del individuo está, por lo tanto, ligado a su capacidad de acceso, gestión y uso de la información. Assange prosigue: "Puedes estar informado y ser tu propio gobernante, o bien puedes vivir en la ignorancia y dejar que otras personas, bien informadas, te gobiernen" (Assange, en Hastings, 2012: 46). Es la misma línea argumentativa que mantiene el hacker Emmanuel Goldstein:

> Creo que podemos imaginarlo mejor si pensamos en nosotros mismos a toda velocidad por una autopista potencialmente peligrosa. Tal vez el camino se convierta en terreno resbaladizo por hielo o esté lleno de peligrosas curvas. Es un camino por el que nadie ha ido antes. Y la pregunta que nos tenemos que hacer es en qué tipo de vehículo preferiríamos estar si las cosas empezasen a estar fuera de control: ¿en nuestro propio automóvil, donde tendríamos al menos alguna posibilidad de controlar el vehículo y ponerlo a una velocidad segura, o en un autobús en el que, junto con muchos otros, debemos poner toda nuestra confianza en un absoluto desconocido para evitar un desastre? La respuesta es obviamente diferente dependiendo de las circunstancias. Hay quienes no quieren la responsabilidad de conducir y hay quienes han demostrado que no son merecedores de ella. Lo importante es que todos tenemos la oportunidad, en algún momento, de elegrir en qué dirección queremos ir. Los cambios tecnológicos rápidos también pueden ser muy peligrosos si no miramos adónde vamos o si muchos de nosotros cerramos los ojos y dejamos que otros nos conduzcan (Goldstein, 2009: 551).

Para los *cypherpunks*, en una época en la que la información circula por redes electrónicas, estas aspiraciones de la cultura hacker son realizables mediante la criptografía robusta, utilizando sistemas de cifrado que permiten al individuo recorrer las redes de información y enviar mensajes de manera segura, esquivando el sistema de vigilancia global. En esto hay consenso:

> La criptografía puede resolver el problema de la interceptación masiva, pues es la interceptación masiva, y no la identificación de objetivos individuales, lo que constituye una verdadera amenaza para la civilización global (Assange *et al*., 2012: 61-62).

Sin embargo, en el seno de esta comunidad existen diferencias ideológicas sustanciales sobre el modelo de sociedad que la alta tecnología debe contribuir a crear.

[140] Las citas tomadas de Forbes (2011) son traducciones propias del texto original, en inglés.

IV.4.2.3.1. Divergencias políticas *cypherpunks*

Al reconocerse como *cypherpunk* (Assange *et al.*, 2012), el fundador de WikiLeaks puede ser inscrito en el ciberanarquismo o, siendo más precisos, en el criptoanarquismo, que básicamente lo que pretende es vaciar de poder al Estado para volcarlo en el individuo. Aquí es donde podemos empezar a dilucidar con más claridad el pensamiento político de Assange y sus ideas sobre el papel que deben jugar gobiernos, empresas y medios de comunicación para asegurar el ideal de libre información.

Robert Manne (2011) —profesor emérito de Política de La Trobe University, en Melbourne— reconoce a casi todos los *cypherpunks* como anarquistas que consideran que el Estado es un enemigo de la libertad; la mayoría, pero no todos, son anarquistas de derechas, es decir, libertarios anarcocapitalistas que apoyan el capitalismo *laissez-faire*. Su gurú es Tim May, brillante exingeniero electrónico de la empresa tecnológica Intel, escritor y autor de *Cyphernomicon* (1994), un documento escrito en el modelo de «preguntas frecuentes» (más conocido en Internet como *FAQ*, acrónimo de *Frequently Asked Questions*) para la lista de correo electrónico *Cypherpunks*. May está considerado "la voz política más autorizada entre los *cypherpunks* libertarios" (Manne, 2011).

En el *Cyphernomicon*, Tim May reconoce a la mayoría de *cypherpunks* como anarcocapitalistas radicales —o criptoanarquistas de derechas—, aunque también deja espacio en este primer grupo de *cypherpunks* a representantes de una derecha más formal y a liberales y libertarios de izquierdas. Todos ellos, sin embargo, comparten la comprensión de la radical importancia política de la criptografía y la voluntad de luchar por la privacidad y la plena libertad del individuo en el ciberespacio. May establece claramente los intereses de los *cypherpunks*: privacidad, tecnología, encriptación, política, criptoanarquía, dinero digital y protocolos (1994: 3.4.2.), siendo la criptoanarquía la consecuencia lógica de una criptografía robusta que permitiría una forma de gobierno basada en acuerdos voluntarios y libres de fuerzas coercitivas externas, leyes y regulaciones (May, 1994: 4.11.1.).

> Algunos de nosotros creemos que diversas formas de criptografía robusta harán disminuir el poder del Estado, tal vez incluso lo hagan colapsar abruptamente. Creemos que la expansión en el ciberespacio, con comunicaciones seguras, dinero digital, anonimato y seudónimos, y otras interacciones mediadas con criptografía,

> cambiarán profundamente la naturaleza de las interacciones económicas y sociales (May, 1994: 2.13.1.)[141].

Los criptoanarquistas representados por May consideran la democracia moderna una "parodia", una "tiranía de las mayorías" que se sustenta en el voto institucionalizado. Esta tiranía debe ser combatida facultando al individuo de nuevas capacidades que le permitan tomar sus propias decisiones morales y romper, mediante la criptografía, las cadenas locales que lo atan a sistemas normativos basados en la autoridad de las mayorías (May, 1994: 4.12.2.). Lo que proponen estos *cypherpunks*, por lo tanto, es la desterritorialización efectiva del individuo y su emancipación del Estado-nación como vertebrador de una identidad común definida por los límites de los espacios geopolíticos, que ha prevalecido sobre la identidad individual, sometida al imperio de la exposición y el escrutinio públicos. En el mundo utópico ideado por May, sólo las elites con habilidades criptotecnológicas prosperarían en un modelo de sociedad meritocrática puro (May, 1994: 6.7.3.).

Los fundamentos criptoanarquistas son formulados por primera vez en el *Manifiesto Criptoanarquista* (*The Crypto Anarchist Manifesto*), que May publicó primero en agosto de 1988 e incluyó más tarde en el *Cyphernomicon*. En éste, aventura una nueva capacidad para comunicarse e interactuar en redes electrónicas de forma totalmente anónima, gracias al reenrutado de paquetes encriptados en máquinas a prueba de manipulación que implementen protocolos criptográficos seguros. Este anonimato garantizado posibilitaría nuevas relaciones sociales y tratos comerciales en los que la reputación y la confianza que ésta genera serían los factores centrales determinantes. Para May, el desarrollo de la criptografía alterará completamente la naturaleza de la regulación del gobierno, su capacidad de gravar y de controlar las interacciones económicas, y su capacidad de guardar información secreta. Hasta aquí, las luces. Porque la de May es una utopía *tenebrista*.

> El Estado intentará, por supuesto, retardar o detener la diseminación de esta tecnología, alegando motivos de seguridad nacional, el uso de esta tecnología por traficantes de drogas y evasores de impuestos, y miedos de desintegración social. Cualquiera de estas preocupaciones serán válidas; la criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinatos y extorsiones. Varios elementos criminales y

[141] Las citas tomadas de May (1994) son traducciones propias del texto original, en inglés.

> extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la extensión de la criptoanarquía. La criptoanarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de púas hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, de igual modo el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de púas alrededor de la propiedad intelectual (May, 1994: 16.4.2.).

Aunque Assange reconoce que los textos fundacionales de WikiLeaks rezuman anarquismo (Manne, 2011) y encontramos en su discurso coincidencias con la retórica criptoanarquista dominante entre los *cypherpunks*, existen diferencias sustanciales que alejan al fundador de WikiLeaks de los principios anarcocapitalistas de May. Principalmente: Assange sí justifica el control selectivo de comunicaciones de individuos y grupos que utilicen tecnología criptográfica para fines criminales —el propio Assange colaboró con la Policía de Victoria (Australia) para acabar con una red de pedofilia en 1993 (Manne, 2011; Butcher, 2011)—, pero entiende también que la existencia de redes de delincuencia en el ciberespacio no puede justificar el control de la tecnología y de la población como medida preventiva contra el crimen. Además, el fundador de WikiLeaks se ha mostrado abiertamente partidario del uso de sutiles mecanismos reguladores del mercado, ha sido crítico en la lista *Cypherpunks* con el capitalismo *laissez-faire* y lo que percibe como una postura ingenua de los anarcopatitalistas, ha defendido el papel de los sindicatos como contrapoder y siempre se ha mostrado partidario del altruismo, de la filantropía y del activismo por los derechos humanos y la justicia social. Por lo tanto, coincidimos con el profesor Manne (2011) en que Assange parece estar más próximo al criptoanarquismo de izquierdas que al anarcocapitalismo de May, aunque una de sus obsesiones ha sido intentar proteger a WikiLeaks de cualquier intento de politizarla en términos de derechas e izquierdas.

Assange admite la influencia que sobre su pensamiento ha tenido la corriente libertaria más radical en lo que se refiere al ideal del libre mercado, aunque con matices:

> No es acertado meterme en un campo filosófico o económico determinado, ya que he aprendido de muchos. Pero uno es el libertarismo norteamericano, el libertarismo de mercado. En lo que a los mercados se refiere, soy un libertario, pero tengo suficiente experiencia en política e historia para comprender que un mercado libre termina siendo un monopolio a menos que se le obligue a ser libre (Assange, en Greenberg, 2010)[142].

[142] Las citas tomadas de Greenberg (2010) son traducciones propias del texto original, en inglés.

Firme anticomunista (Manne, 2011), el fundador de WikiLeaks mantiene, sin embargo, una postura escéptica sobre el capitalismo, aunque rehúye de la etiqueta de anticapitalista. Assange reconoce que le encantan los mercados, pero considera necesaria su regulación mediante mecanismos fiscalizadores independientes para asegurar su libertad y extirpar del sistema la corrupción, el abuso de poder, las trampas, la especulación, la conspiración, el secreto, el fraude o la evasión de dinero a paraísos fiscales: "No soy un gran fan de la regulación; cualquier persona a la que le guste la libertad de prensa no lo puede ser. Pero hay algunos abusos que deben ser regulados" (Assange, en Greenberg, 2010). Y ése es precisamente el papel que otorga a WikiLeaks, el de una fuerza reguladora de gobiernos, de empresas privadas y de sus contubernios, de manera que esa "amenaza de regulación" es la que "produce la autorregulación", la que "hace el capitalismo más libre y ético" (Assange, en Greenberg, 2010).

Alejado de propuestas extremistas dirigidas a destruir el sistema, lo que busca Assange es iniciar la catarsis del mismo para alcanzar su perfección; o visto de otra manera: hackear el *sistema operativo* del mundo para mejorarlo. Assange se confiesa partidario del libre mercado entendido como manifestación sublime de un flujo de información perfecto, esto es, libre. La transparencia y el conocimiento son la base para alcanzar este ideal de un mercado auténticamente libre y de libre competencia en igualdad de condiciones. Para que un mercado sea libre, dice, "la gente tiene que saber con quién están tratando" (Assange, en Greenberg, 2010).

Por último, frente al *darwinismo* tecnológico proclamado por May y los anarcocapitalistas, Assange, aunque no niega que sólo los individuos tecnológicamente más formados y habilidosos tendrían la posibilidad de evadir el control corporativo-estatal y la capacidad de conservar su libertad en una sociedad globalmente vigilada (Assange *et al.*, 2012: 1, 161), considera que esas habilidades deben ser mostradas y facilitadas por las elites tecnológicas —los intelectuales de nuestro tiempo— a todos los individuos, para organizar de un modo más eficiente la producción intelectual humana y una nueva estructura social en pro del bien común, no sólo de unas elites meritocráticas. En definitiva, su objetivo principal "no es crear un sistema que premie mejor a los individuos innovadores", sino "interrumpir lo que él ve como prácticas conspirativas de instituciones sólidas (es decir, instituciones con fuertes barreras contra el flujo de información)" (Jurgenson y Rey, 2014: 2657-2658).

IV.4.2.3.2. Las tres libertades básicas: movimiento, comunicación e interacción económica

Desde principios de la década de 1990, el *cypherpunk* radicalizó el debate público sobre las tensiones entre el Estado-nación y el individuo, que Assange identifica como la colisión entre las tres características básicas del Estado y las tres libertades fundamentales que los *cypherpunks* reclaman para el individuo, de las que derivarían todas las demás libertades (Assange *et al.*, 2012: 88), esto es: 1) el control estatal ejercido con fronteras físicas *vs* la libertad de movimiento en un espacio desterritorializado, 2) el control estatal de las comunicaciones *vs* la comunicación privada, y 3) el control corporativo-estatal de las actividades económicas *vs* la libertad de interacción económica. La consecución de esta última libertad —que está intrínsecamente ligada a la libertad de expresión para los *cypherpunks* estadounidenses, no tanto para los europeos, según Appelbaum (Assange *et al.*, 2012: 102)— sería la culminación de la emancipación del individuo. Y esto pasa por liberar la infraestructura de las comunicaciones electrónicas del control del poder corporativo-gubernamental.

Andy Müller-Maguhn arguye:

> […] si el sistema económico está basado en la infraestructura electrónica, la arquitectura de la infraestructura electrónica nos dice algo sobre cómo se produce el flujo de dinero, sobre cómo está siendo controlado y cómo está siendo centralizado. […] la arquitectura de la tecnología se está convirtiendo en un asunto clave, pues afecta a todos los demás campos, y eso es lo que realmente tenemos que redefinir, en el sentido de que si queremos contar con un sistema descentralizado de gestión de nuestros pagos, necesitamos tener la infraestructura en nuestras manos (Assange *et al.*, 2012: 96).

Al respecto, Assange expone que para desmantelar la estructura de control estatal sobre las interacciones económicas es necesario romper el monopolio monetario que los Estados ejercen mediante los bancos centrales como emisores únicos de moneda; un modelo monetarista estrechamente ligado al constructo de nación y sus límites territoriales, que se opone a la lógica libertaria ciberespacial. Por eso, los *cypherpunks* apoyan el uso de nuevas monedas virtuales, de criptomonedas como Bitcoin, cuyo uso generalizado contribuiría al final del Estado-nación.

> Si eliminas este monopolio estatal sobre los medios de interacción económica, entonces eliminas uno de los tres componentes del Estado. En el modelo de Estado concebido como una mafia, el Estado ejerce de extorsionador, registrando a las personas en busca de dinero de todos los modos posibles. Controlar los flujos de dinero es importante para incrementar los ingresos del Estado, pero también para controlar lo que

> la gente hace: incentivar una cosa, desincentivar otra, prohibir totalmente ciertas operaciones, o una organización, o las interacciones entre organizaciones. De modo que, por ejemplo, lo que ocurrió con el insólito bloqueo a WikiLeaks no fue fruto de una decisión del libre mercado, pues no tenemos un libre mercado: las legislaciones estatales han convertido a determinados actores financieros en reyes y no permiten la entrada de nuevos actores. La libertad económica ha sido vulnerada por una elite capaz de influir tanto en la normativa como en los principios que rigen estos bancos (Assange *et al.*, 2012: 92).

Los *cypherpunks* fueron pioneros en proponer y apoyar los primeros sistemas criptográficos libres *peer-to-peer* para hacer pagos, como la moneda *chaumiana*, el eCash, la primera divisa electrónica anónima, diseñada en la primera mitad de la década de 1990 conforme a las especificaciones propuestas por el criptógrafo holandés David Chaum en 1983. La idea era crear una moneda electrónica contraria a los sistemas de rastreo y seguimiento que permiten las transacciones con Visa o MasterCard, por ejemplo. Sin embargo, la moneda *chaumiana* se emitía de manera centralizada. Este hándicap fue resuelto en 2009 con la aparición de Bitcoin, otra criptomoneda electrónica que permite un sistema de transacciones públicas, pero anónimas y sin autoridad central. Bitcoin es la primera implantación realmente exitosa de una idea clásica del movimiento *cypherpunk*: la moneda criptográfica digital. Una nueva ética bancaria que nos acerca al ideal del libre mercado *cypherpunk*, sostenido en un sistema de confianza distribuida que, según sus defensores, dificulta el fraude (Assange *et al.*, 2012: 97-98).

Lo que subyace, por lo tanto, en el movimiento *cypherpunk* es un intento de configurar un nuevo modelo económico, un nuevo sistema de economía de libre mercado en un sentido mucho más profundo y efectivo que en el léxico capitalista tradicional, pero sin dejar de ser economía capitalista. Para los *cypherpunks*, el auténtico libre comercio permitiría alcanzar el grado superior de libertad, supondría la culminación de la plena emancipación y soberanía del individuo, fruto de la consecución de las dos primeras libertades básicas, las de movimiento y comunicación (Assange *et al.*, 2012: 87-88).

Para Julian Assange, las tres características fundamentales sobre las que el Estado vertebra su poder autoritario son: el control de una fuerza armada en una región concreta, una infraestructura de comunicaciones también controlada y una infraestructura financiera (Assange *et al.*, 2012: 87). En oposición a estos tres pilares del

Estado, el fundador de WikiLeaks define así las "tres libertades básicas" para el individuo:

> La libertad de movimiento, la libertad física de movimiento: la capacidad de movernos de un sitio a otro sin tener un ejército pisándonos los talones. En segundo lugar, podemos pensar en la libertad de pensamiento y en la libertad de comunicación, la cual es inherente a la libertad de pensamiento: si sufres amenazas por expresarte públicamente, la única manera de salvaguardar tu derecho a comunicarte es hacerlo privadamente. Y, finalmente, la libertad de interacción económica, que al igual que la libertad de comunicación, también está indisolublemente unida a la privacidad de la interacción económica" (Assange *et al.*, 2012: 87-88).

En la transición de la sociedad global a la Red, la libertad de movimiento ha seguido siendo, en esencia, la misma; la libertad de comunicación se ha ampliado en cuanto a nuestra capacidad de interactuar con más personas, pero a cambio de perder privacidad y de ceder nuestros datos al poder corporativo-gubernamental para que los almacene y explote, y lo mismo ha sucedido con nuestras interacciones económicas, almacenadas en servidores (Assange *et al.*, 2012: 87-88). Los límites y controles sobre nuestras comunicaciones e interacciones económicas redundan en perjuicio de la libertad de movimiento (Assange *et al.*, 2012: 96). Un ejemplo de esto son los sistemas de geolocalizacion móvil, normalizados en las comunicaciones electrónicas para facilitar el rastreo de nuestras localizaciones.

Los sistemas de geolocalización, liberados para su uso masivo e instalados en nuestros dispositivos electrónicos móviles, están contribuyendo, por ejemplo, a mejorar los servicios de rescate y de emergencias, o a resolver casos de secuestros, pero también favorecen la normalización del panoptismo ciberespacial, estandarizando prácticas de control y vigilancia de individuo a individuo (por ejemplo, sistemas de vigilancia para los padres que quieren controlar permanentemente la ubicación de sus hijos mediante estos sistemas), de empresa a individuo (por ejemplo, la explotación comercial que las empresas hacen de nuestras comunicaciones geolocalizadas voluntariamente en redes sociales en línea) y de gobierno a individuo (por ejemplo, el rastreo de las comunicaciones electrónicas de un individuo investigado, para trazar sus movimientos y localizar su ubicación). Los sistemas de geolocalización se han convertido en un arma de doble filo en un mundo de vigilancia global en el que todos podemos ser vigilantes y vigilados, y contra el que los *cypherpunks* proponen una solución tecnológica: el cifrado de nuestras comunicaciones como instrumento para garantizar nuestra plena libertad.

La gravedad es real. En el informe *The right to privacy in the digital age*, fechado el 30 de junio de 2014, la alta comisionada de Naciones Unidas para los Derechos Humanos, Navanethem Pillay, alerta de un incremento de las prácticas nacionales y extraterritoriales de vigilancia electrónica y de recolección y almacenamiento de datos personales. El documento denuncia además la opacidad con la que se opera, con una "preocupante falta de transparencia gubernamental" que impide cualquier intento de evaluar la coherencia de estas prácticas —amparadas por leyes nacionales— con las normas internacionales de derechos humanos y que dificulta que se asuman responsabilidades (Pillay, 2014: 16).

El organismo supanacional advierte también de que los programas de vigilancia masiva, así como la interceptación de comunicaciones digitales y la recolección y el almacenamiento de datos personales, no sólo pueden infringir el derecho a la privacidad, sino también otros derechos fundamentales como el derecho a la libertad de opinión y de expresión, el derecho a buscar, recibir y difundir información, el derecho de libertad de reunión y de asociación pacíficas, o el propio derecho a la vida familiar, todos ellos estrechamente vinculados al derecho a la privacidad. También el derecho a la salud puede verse afectado por las prácticas de vigilancia digital, por ejemplo, cuando un individuo, por temor a que su anonimato se vea comprometido, se abstiene de buscar o comunicar información sensible relacionada con un problema de salud personal (Pillay, 2014: 5).

El Alto Comisionado de Naciones Unidas también asegura que "existen indicios creíbles que sugieren que las tecnologías digitales se han utilizado para obtener información que luego ha llevado a tortura y otros malos tratos", así como informes que "también indican que metadatos obtenidos de la vigilancia electrónica han sido analizados para identificar la ubicación de objetivos para ataques aéreos letales" (Pillay, 2014: 5).

El organismo no excluye de responsabilidades a las compañías tecnológicas que proveen infraestructuras y servicios para las comunicaciones digitales. El Alto Comisionado considera que, si bien un Estado puede tener razones legítimas para requerir a estas empresas información y datos de usuarios, estima que las compañías corren el riesgo de ser cómplices y partícipes de abusos de derechos humanos cuando la suministración de esa información y datos contraviene el derecho a la privacidad o

compromete la seguridad de individuos allí donde la información se controla para violar derechos humanos (Pillay, 2014: 15).

Además, se adviere de que el uso de las tecnologías de monitorización y recolección masiva de datos se están aplicando también en el mercado global, "aumentando el riesgo de que la vigilancia digital escape a los controles gubernamentales" (Pillay, 2014: 3).

El reporte de la Alta Comisionada de Naciones Unidas confirma las denuncias que en los últimos años han hecho hackers y hacktivistas, acredita las revelaciones de documentos sobre los sistemas de vigilancia nacionales y global, y refuerza las críticas al uso de estos mecanismos sin controles judiciales ni criterios de excepcionalidad ni proporcionalidad racionales.

IV.4.2.3.3. De la distopía *orwelliana* a la utopía libertaria *cypherpunk*

La Red se ha convertido en el escenario central de las tensiones entre la utopía libertaria de la emancipación del individuo y la distopía *orwelliana* de una sociedad totalmente dependiente de gobiernos y grandes corporaciones que trafican con información y la ocultan para controlar con mayor facilidad a las masas. En plena lucha dialéctica entre individuo e imperio corporativo-gubernamental, entre privacidad y vigilancia, entre transparencia y secreto, entre libertad y seguridad, el interés de Julian Assange es superar la retórica distópica que ha prevalecido sobre los impulsos utópicos en el debate público.

El acto más subversivo de Assange —y por ende, de WikiLeaks— ha sido tomarse en serio y dirigir contra el sector corporativo y el Estado-nación la advertencia que en 1999 lanzó Scott McNealy, consejero delegado de Sun Microsystems: "Tienes cero privacidad. Asúmelo" (Andrejevic, 2014: 2619). Partiendo de este aserto, que nos coloca en un escenario distópico, Assange articula su discurso con el ánimo de agitar conciencias.

> El mundo no se está deslizando, sino que va al golope hacia una nueva distopía transnacional. Este desarrollo no ha sido debidamente reconocido fuera del ámbito de la seguridad nacional. Se ha ocultado por su confidencialidad, complejidad y escala. Internet, nuestra mayor herramienta de emancipación, ha sido transformada en la más peligrosa herramienta para el totalitarismo que hemos visto nunca. Internet es una amenaza para la civilización humana.

> Estas transformaciones han ocurrido en silencio, porque los que saben lo que está pasando trabajan en la industria de la vigilancia y no son incentivados para denunciar. De seguir este rumbo, dentro de unos pocos años la civilización mundial será una distopía posmoderna de vigilancia, de la cual será para todos imposible escapar, excepto para los individuos más habilidosos. De hecho, puede que ya estemos ahí. (Assange *et al.*, 2012: 1).

A partir de aquí, y aceptando que la antiutopía se está materializando, Assange sugiere no recrearse en escenarios pesimistas y propone a sus colegas de las nuevas generaciones *cypherpunks* un ejercicio de imaginación sobre un escenario utópico que supere la nebulosidad distópica. La mera queja sobre la creciente vigilancia resulta inútil para Assange; no vale de nada. El tránsito de la distopía *orwelliana* a la utopía libertaria solamente será posible imaginando su materialización y adoptando una actitud proactiva que se concrete en la construcción de las herramientas necesarias para una nueva democracia protegida y apuntalada por la alta tecnología.

> […] podemos construirlas con nuestras mentes, difundirlas a otra gente e involucrarnos en la defensa colectiva. La tecnología y la ciencia no son algo neutral. Hay formas concretas de tecnología que nos pueden suministrar estos derechos y libertades fundamentales tan anhelados por muchos desde hace tanto tiempo (Assange *et al.*, 2012: 151).

En el tránsito de la distopía materializada a la utopía realizable, Müller-Maguhn estima que será clave afianzar procesos de transparencia informativa, pero también mecanismos internos de denuncia en empresas privadas y en instituciones públicas que garanticen la seguridad de los denunciantes. Zimmermann, por su parte, considera que "una Internet libre, abierta y universal es probablemente la herramienta más importante que tenemos para resolver los problemas globales que están en juego", por lo que "protegerla es posiblemente una de las tareas claves que nuestra generación tiene entre manos" (Assange *et al*., 2012: 150). Mientras que para Appelbaum la utopía se materializará en el derecho a conocer y el derecho a expresarse libremente, sin excluir a un solo ser humano, sin excepciones de ningún tipo:

> De ahí se deriva el derecho a la expresión anónima, el derecho que te permite pagar a cualquier persona sin interferencias de terceros, la capacidad de viajar libremente, la capacidad de corregir la información que sobre ti aparece en los sistemas. Contar con sistemas transparentes a los que podamos pedir cuentas cuando observemos algún tipo de intromisión (Assange et al., 2012: 149).

En resumen, los nuevos *cypherpunks* inciden en la necesidad de incrementar el coste político para aquéllos que intenten por cualquier medio controlar la Red, en explorar nuevas vías de intercambio de conocimiento y de acción, y en "desarrollar herramientas para capacitar mejor a los ciudadanos en la construcción de sus propias infraestructuras encriptadas y descentralizadas, para que puedan ser dueños de sus propias infraestructuras de comunicación" (Assange *et al.*, 2012: 151).

IV.5. ESTRATEGIA DE COMUNICACIÓN: MÁXIMO IMPACTO MEDIÁTICO Y POLÍTICO

IV.5.1. Introducción

La existencia de WikiLeaks abre nuevos escenarios de acceso universal y masivo a la información en bruto por parte de los ciudadanos, sin que los datos pasen por el filtrado de los medios de información tradicionales, cuestionando así su papel de mediadores informativos en la sociedad y poniendo en duda el modelo de mercantilización de la información que impera. Sin embargo, WikiLeaks renunció a sus principios con motivo del caso *Cablegate*, cuando Julian Assange decidió que los medios tradicionales de masas deberían jugar un papel clave en la difusión de su mensaje, concediéndoles legitimidad como intermediarios necesarios.

Asimismo, las filtraciones masivas de documentos secretos se enmarcan en las nuevas estratégicas para desactivar la conspiración como forma de gobierno. Antes de diseccionar la estrategia mediática de WikiLeaks creemos que es necesario explicar su estrategia política para desactivar el secreto como mecanismo de gobierno, desarrollada teóricamente por Assange en sus ensayos políticos publicados durante la gestación de WikiLeaks.

IV.5.2. Filtraciones masivas para desactivar la conspiración

La base teórica y conceptual sobre la que Assange ha construido su *ser* político le ha llevado a identificar el Estado como enemigo y principio de la mentira. Un aspecto interesante y clave en el pensamiento de Assange es que extiende la idea de Estado a las corporaciones empresariales, aliadas de los gobiernos; poderes cómplices para dominar el mundo, como señala el fundador de WikiLeaks en su breve ensayo *Conspiracy as Governance* (2006).

En la teoría política de Assange se observa una radical y crítica visión del imperio corporativo-gubernamental, especialmente centrada en la realidad estadounidense, donde los poderes corporativos configuran, según Assange, "una especie de federación de estados comunistas" a la que denomina, con causticidad, "Unión Soviética de América", en un artículo publicado en su blog personal, el 9 de junio de 2007, con el título 'The United what of America?' (Assange, 2006-2007).

Palabras que recuerdan a las ya mencionadas del gurú hacker Richard Stallman: "Tenemos un nivel de vigilancia general mucho mayor que el que existía en la Unión Soviética" (Richard Stallman, en Quian, 2013c).

La coalición conspirativa entre el poder político corrompido y el poder económico corruptor fue diseccionada por Julian Assange en su breve ensayo *Conspiracy as Governance* —el eje teórico de WikiLeaks—, publicado el 3 de diciembre de 2006, coincidiendo con el nacimiento de esta organización. Este ensayo político forma parte de la etapa —entre julio de 2006 y agosto de 2007— en la que Assange articuló su retórica contra el control y vigilancia del Estado, en una serie de textos publicados en su blog *IQ.org* (IQ: Interesting Question), ahora desactivado, aunque aún accesible en la Red en la base de datos Wayback Machine, que almacena copias de sitios web.

En esta serie de anotaciones personales y breves ensayos, unificados bajo el epígrafe *Selected Correspondence*, se encuentran las bases filosóficas del tratado teórico de WikiLeaks. Aquí, Assange ya alude a los efectos de las filtraciones de información en sistemas de gobierno herméticos e injustos. En un breve texto titulado 'The non linear effects of leaks on unjust systems of governance', publicado el 31 de diciembre de 2006, dice: "Cuanto más secreta o injusta es una organización, más miedo y paranoia inducen las filtraciones en su liderazgo" (Assange, 2006-2007).

Una de las revelaciones más sustanciales de estos textos personales es la mentalidad estratégica de Julian Assange, no sólo en lo que respecta a la ejecución de nuevas tácticas de resistencia tecnológica y a la desarticulación de los vínculos entre conspiradores, sino también —y he aquí lo más novedoso— en la consecución del mayor impacto político posible mediante el flujo libre de información. Assange, interesado en los programas informáticos en desarrollo para las comunicaciones seguras, advierte que proyectos como Freenet —anterior a WikiLeaks— es un intento estéril de construir una red de distribución de información descentralizada y resistente a la censura.

Freenet es el resultado de un proyecto del científico computacional Ian Clarke presentado en 1999 en la University of Edinburh con el título *A Distributed, Decentralised Information Storage and Retrieval System*. En este documento, de cuarenta y tres páginas, su autor describe así su algoritmo:

> […] si se ejecuta por un grupo de nodos interconectados, proporcionará un robusto sistema de almacenamiento y recuperación de información indexada sin ningún elemento de control central o administración. Permite que la información esté disponible para un gran grupo de personas de una manera similar a la de la World Wide Web (Ian Clarke, 1999: Abstract).

El algoritmo permite, además, que la publicación y recuperación de información sean anónimas.

Clarke llevó sus ideas a la práctica en el año 2000, cuando lanzó Freenet, un proyecto de software libre para proteger la libertad de expresión, facilitando el intercambio seguro de archivos, la publicacón y recuperación anónimas de información y la participación en foros de discusión sin temor de censura[143]. Sin embargo, el fundador de WikiLeaks encuentra una falla en Freenet, en concreto, en sus foros, cuyo impacto político, dice, es nulo, ya que sólo parecen eficaces "para usuarios muy altamente motivados" (Assange, 2006-2007).

Julian Assange piensa en cómo se pueden generar situaciones que motiven a cualquier individuo a actuar con coraje, es decir, a revelar información secreta de gobiernos y corporaciones empresariales y financieras. Es así como, inspirado en proyectos como Cryptome y Freenet, da con la idea de WikiLeaks como instrumento motivador para desactivar los vínculos conspirativos que alimentan al poder autoritario. Fundamentalmente, la teoría de Assange sostiene que los poderes autoritarios se valen de la conspiración y del secreto para mantener y fortalecer sus estructuras, impidiendo la existencia de un buen gobierno basado en la justicia y la verdad. Una idea que desarrolla en *Conspiracy as Governance*:

> Allá donde se conocen detalles del funcionamiento interno de los regímenes autoritarios, vemos interacciones conspirativas entre la elite política, no sólo por obtener preferencias o favores dentro del régimen, sino como la principal metodología de planificación para mantener o fortalecer el poder autoritario.
>
> Los regímenes autoritarios hacen surgir fuerzas que se oponen a ellos, al intentar refrenar las ganas de verdad, amor y autorrealización de un pueblo. Los planes de los que se vale el gobierno autoritario, una vez descubiertos, causan mayor resistencia. De ahí que los poderes autoritarios que triunfan oculten tales planes hasta que la resistencia es inútil o se ve superada por la eficiencia del poder bruto. Este secretismo colaborativo, que actúa en perjuicio de la población, es suficiente para definir sus comportamientos como conspirativos (Assange, 2006: 2)[144].

[143] Disponible en: https://freenetproject.org/ (último acceso: 22 de mayo de 2015).
[144] Las citas tomadas de Assange (2006) son traducciones propias del texto original, en inglés.

La conspiración es, para Assange, un artilugio cognitivo que se ejectuta entre un cúmulo de individuos que intercambian rápidamente información adquirida del medio en el que operan (entorno conspiratorio), para beneficio de los miembros de este grupo excluyente y en detrimento del grupo excluido. En caso de arreglo, los individuos del grupo excluyente erigen barreras entre ellos y el grupo excluido, con el fin de consolidar y asegurar aún más su arreglo beneficioso. Assange explica:

> Podemos ver las conspiraciones como un tipo de artefacto que tiene sus *inputs* (la información sobre el entorno), una red de procesamiento de datos (los conspiradores y los vínculos que los unen) y sus *outputs* (las acciones destinadas a cambiar o mantener el entorno) (Assange, 2006: 3).

La información fluye de conspirador a conspirador en una estructura en red configurada por algunos nodos centrales vinculados a muchos conspiradores, por otros menos poderosos y periféricos que se vinculan con unos pocos, y también por nodos que actúan como intermediarios, es decir, como vínculos entre otros conspiradores (Assange, 2006: 2).

En Assange, la importancia de los vínculos entre conspiradores se mide por su *peso*, es decir, por la cantidad de comunicación importante que fluye por éstos.

> Simplemente decimos que la «importancia» de la comunicación contribuye al peso de un vínculo de la manera más obvia: el peso de un vínculo es directamente proporcional a la cantidad de comunicación importante que fluye por él (Assange, 2006: 3)

La prioridad del hacktivista debe ser, por lo tanto, dañar los vínculos, no atacar física o virtualmente a los conspiradores. Por supuesto, la conspiración ha existido antes de la sociedad red, pero el paradigma informacionalista ha contribuido a que ésta se dilate y sus flujos de información se aceleren en una Red de redes global. La conspiración, como artefacto, se ha digitalizado, aumentando casi infinitamente los *inputs* con la obtención masiva de información y datos, ampliando la extensión y capacidad de su red de procesamiento, y mejorando y expandiendo mundialmente su capacidad de acción, en un ambiente conspitativo global. Para este este nuevo escenario, Assange argumenta que los ataques tradicionales a los grupos de poder conspirativos —como la intimidación, el chantaje, el secuestro o el asesinato— no son útiles, pues son "el resultado de inclinaciones mentales desarrolladas para las sociedades analfabetas"

(Assange, 2006: 5). El desarrollo de redes electrónicas y de tecnologías digitales de comunicación y procesamiento masivo de información y datos, han dotado a los conspiradores de nuevos medios que han incrementado la velocidad y precisión de sus interacciones y, en consecuencia, el tamaño de la conspiración y el poder de quienes conspiran; pero también mejora la resistencia a los conspiradores y favorece asaltos más eficaces a su red de procesamiento para atacar el proceso mismo que conduce a la conspiración, es decir, a su capacidad cognitiva. Si los vínculos entre conspiradores se debilitan o rompen y los conspiradores dejan de controlar la información, pierden su ventaja. Pero, ¿cómo?

> Podemos *engañar* o *cegar* a la conspiración restringiendo o distorsionando la información de la que dispone.
>
> Podemos reducir el *poder conspirativo total* con ataques desestructurados a los vínculos o mediante *estrangulamiento* y *división*.
>
> Una conspiración suficientemente comprometida de esta manera ya no es capaz de comprender su entorno ni planear una acción robusta (Assange, 2006: 5).

Veamos sucintamente ahora cómo se aplica este modelo teórico a las filtraciones de WikiLeaks: si el flujo de secretos entre conspiradores es interrumpido o intervenido parcial o totalmente, la trama conspirativa es dañada. El nivel del daño causado dependerá de la cantidad de información afectada, que nos da una medida de la magnitud de los conspiradores y de sus conspiraciones, o viceversa; esto es: cuanto mayor sea el flujo de información secreta que manejan, más poderosos son los conspiradores y más relevante es su interceptación. Pero aún más importante es la revelación pública de esos secretos para debilitar a los nodos centrales de la conspiración y, con ellos, a toda la red conspirativa, o al menos a la parte más importante. Esto podría explicar por qué WikiLeaks ha pasado de la interceptación de pequeños flujos de información secreta —mucha de ésta, de nodos periféricos (pongamos, por ejemplo, corrupción política en países africanos)— a una estrategia que prioriza las filtraciones masivas de secretos que afectan a los nodos centrales de una red de conspiración con efectos globales (principalmente, el Gobierno de Estados Unidos y sus aliados).

Así, el impacto mediático y político que puedan tener las revelaciones de un puñado de documentos secretos de la Iglesia de la Cienciología, de la Policía keniata o del banco Julius Bär no será el mismo que el que alcancen las publicaciones de un

cuarto de millón de cables diplomáticos de Estados Unidos, de casi medio millón de documentos militares confidenciales de las guerras de Irak y Afganistán, o de cinco millones y medio de correos electrónicos de una agencia de inteligencia global.

Uno o varios documentos filtrados sobre corrupción pueden acabar con la carrera de un político o de un empresario; la revelación de un vídeo del asesinato de civiles por soldados, o de fotos de torturas en prisiones militares, puede conseguir juicios militares, tal vez alguna dimisión o el cese de algún alto cargo del Estado, y un eventual debate público sobre derechos humanos sujeto a la agenda de los medios de comunicación de masas. Sin embargo, el hackeo de toda una base de datos gubernamental y la revelación de todos sus archivos secretos es un golpe no a una conspiración, sino al proceso conspirativo y, por lo tanto, a la estructura del poder autoritario; un golpe al propio sistema.

Explicaremos ahora cómo evolucionó la estrategia de WikiLeaks para alcanzar el mayor impacto posible en la opinión pública y debiltar el Estado de secreto.

IV.5.3. Evolución de la estrategia de difusión de las filtraciones

IV.5.3.1. 2006-2010. Autonomía editorial

WikiLeaks se creó en diciembre de 2006 y su página web empezó a operar en enero de 2007, alojada en servidores en Suecia, país donde las leyes protegen el anonimato. Su fundador es Julian Assange y está gestionada por el grupo The Sunshine Press[145]. WikiLeaks era un proyecto en el que Assange llevaba años pensando; no en vano, en 1999 ya había registrado el dominio leaks.org. Según el propio Assange, "la creación de WikiLeaks fue, en parte, una respuesta a lo de Irak":

> La guerra de Irak ha sido el tema más importante para la gente de mi generación en Occidente. También ha sido el caso más claro, que yo recuerde, de manipulación mediática y de creación de una guerra gracias a la ignorancia (Assange, en Hastings, 2012: 48).

Pero el objetivo ulterior era mucho más ambicioso, como evidencia la primera descripción que se ofreció de WikiLeaks. El 3 de enero de 2007, Assange empezó a

[145] En noviembre de 2010, WikiLeaks registró en Islandia su primera entidad legal conocida: Sunshine Press Productions.

preparar una presentación escrita para su publicación en medios de comunicación, tras revelarse prematuramente la existencia de WikiLeaks. Con una retórica deliberadamente pretenciosa y atractiva para la prensa —así lo reconoce el propio Assange en la lista de correo creada en diciembre de 2006 para diseñar, junto con sus colaboradores, el nacimiento de WikiLeaks—, el fundador de la organización describió en aquellos días:

> WL [Wikileaks] puede convertirse en la agencia de inteligencia más poderosa del mundo, una agencia de inteligencia de la gente. […] No tendrá intereses comerciales o nacionales; sus únicos intereses serán la verdad y la libertad de información. […] WL será un yunque en el que golpea el martillo de la conciencia colectiva de la humanidad. […] WL, esperamos, será una nueva estrella en el firmamento político de la humanidad (WikiLeaks Leak, 2007).

La organización ya había empezado a operar por entonces, pero el proyecto se llevaba con discreción. A finales de 2006 y primeros días de 2007, nadie, salvo su grupo fundador, conocía WikiLeaks, hasta que uno de los individuos invitados por Assange para colaborar con él decidió revelar y explicar al mundo la existencia y los objetivos de esta organización. El 3 de enero de 2006, Steven Aftergood publicó en su blog *Secrecy News* —especializado en la política del secreto y alojado en el sitio web de la Federation of American Scientists (FAS)— la primera mención pública a WikiLeaks en un medio de comunicación, en un artículo que título 'Wikileaks and Untraceable Document Disclosure'. La entrada de WikiLeaks en la esfera pública fue controvertida: primero, porque reconfiguraba la agenda de Assange para presentar en público WikiLeaks; segundo, porque era la primera filtración que sufría la organización y abrió la primera fisura en ésta, y tercero, porque supuso también el primer ataque directo contra WikiLeaks.

El perfil de Steven Aftergood era atractivo para Assange. Aftergood es el director del FAS Project on Government Secrecy, dirigido a reducir el alcance del secreto de Estado y a promover el acceso público a la información gubernamental. En 1997 ganó una demanda contra la Agencia Central de Inteligencia de Estados Unidos —la CIA— que obligó a desclasificar y publicar el presupuesto total de inteligencia de Estados Unidos para aquel año: 26.600 millones de dólares. En 2006, ganó otra demanda contra la Oficina Nacional de Reconocimiento para la liberación de sus registros presupuestarios sin clasificar. Aftergood ha sido reconocido con el Pioneer Award de la Electronic Frontier Foundation (2010), el James Madison Award de la

American Library Association (2006), el Public Access to Government Information Award de la American Association of Law Libraries (2006) y el Hugh M. Hefner First Amendment Award de la Playboy Foundation (2004). Sin embargo, rechazó la invitación a participar en el consejo asesor de WikiLeaks y escribió y publicó en su blog lo que para los miembros de WikiLeaks debió ser una respuesta privada sólo dirigida a ellos:

> WikiLeaks invitó a *Secrecy News* a formar parte de su consejo asesor. Le explicamos que no estamos a favor de la publicación automatizada o indiscriminada de registros confidenciales (Aftergood, 2007)[146].

En la que es la primera descripción de WikiLeaks fuera de WikiLeaks, Aftergood presenta "una nueva iniciativa en Internet" que "busca promover el buen gobierno y la democratización posibilitando la divulgación y publicación anónimas de registros gubernamentales confidenciales" (Aftergood, 2007). El sitio web de WikiLeaks ya estaba operativo en aquel momento, pero sólo parcialmente; no era funcional y su enlace no se había distribuido. Aftergood reveló al mundo su existencia y sus fines, tomando el propio texto volcado en la página de WikiLeaks, que describía el proyecto como "una versión incensurable de Wikipedia para la filtración masiva de documentos y su análisis de manera no rastreable" (Aftergood, 2007). Un texto que establecía las bases políticas de la organización, en defensa de derechos fundamentales y del bien común, como cita Aftergood:

> Un sistema [que] permite a cualquier persona filtrar de forma segura a un público preparado es el medio más rentable para la promoción del buen gobierno en la salud y la medicina, en el suministro de alimentos, en los derechos humanos, en el control de armas y de las instituciones democráticas (Aftergood, 2007).

Wikileaks ya presumía de contar con veintidós personas involucradas en el proyecto y de guardar 1,1 millones de documentos que se estaban preparando para su publicación (WikiLeaks Leak, 2007). El primero de ellos ya había sido publicado en un archivo accesible en su sitio web: un documento supuestamente escrito por el jeque Hassan Dahir Aweys, de la Unión de Tribunales Islámicos de Somalia. El llamado *Union of islamic courts.zip*[147] se publicó el 28 de diciembre de 2006, según consta en

146 Las citas tomadas de Aftergood (2007) son traducciones propias del texto original, en inglés.
147 El archivo aún es accesible en: https://www.wikileaks.org/wiki/Union_of_islamic_courts.zip (último acceso: 12 de septiembre de 2015).

los registros de WikiLeaks. Fue su primera publicación de documentos secretos: una carpeta que contiene tres fotografías en formato JPG del documento original y un texto en formato DOC con la traducción en inglés del documento firmado por Hassan Dahir Aweys el 9 de noviembre de 2005. Según los metadatos que hemos leído tras descargar el archivo de la página web de WikiLeaks, los documentos digitalizados fueron creados el 15 de diciembre de 2006 (véase Anexo XXIII).

La publicación en bruto de documentos confidenciales, sin editar y sin control, es una práctica rechazada por Aftergood:

> En ausencia de una supervisión editorial responsable, la publicación puede más fácilmente convertirse en un acto de agresión o en una incitación a la violencia, por no hablar de una invasión de la privacidad o un atentado contra el buen gusto (2007).

Este argumento ya había sido contestado en las comunicaciones privadas que Aftergood había mantenido con los miembros de WikiLeaks, quienes le acusaron de querer imponer la censura: "Los puestos consultivos son sólo eso, ¡consultivos! Si desea asesorarnos para censurar, entonces que sea así" (Aftergood, 2007)

Esta revelación al mundo de la existencia y de las esencias de WikiLeaks obligó a Julian Assange a actuar con premura, ante la previsible reacción periodística que suscitaría el artículo de Steven Aftergood. El 3 de enero de 2007, los miembros de WikiLeaks acordaron por escrito una serie de explicaciones públicas sobre la organización. En éstas, se describe a WikiLeaks como una organización formada por disidentes chinos, expatriados rusos, refugiados tibetanos, periodistas, matemáticos, un exanalista de inteligencia estadounidense, criptógrafos y tecnólogos de todo el mundo (WikiLeaks Leak, 2007). Y aunque la idea original era centrarse en actuar contra regímenes totalitarios no occidentales, la misión de WikiLeaks no tardó en ampliarse para intentar publicar documentos filtrados por fuentes anónimas sobre comportamientos poco éticos y delitos de gobiernos, ejércitos y grandes corporaciones financieras y empresariales de todo el mundo, también de Occidente, en países democráticos. Aftergood recoge la declaración de intenciones de WikiLeaks:

> Nuestros objetivos principales son regímenes altamente opresivos en China, Rusia, Eurasia central, Medio Oriente y África subsahariana, pero también esperamos ser de ayuda a aquellos que en Occidente desean revelar el comportamiento poco ético de sus gobiernos y corporaciones (Aftergood, 2007).

Henry Poole —cofundador de CivicActions, firma que presta servicios para el cambio social a gobiernos y organizaciones sin ánimo de lucro— parece ser el primer eslabón de una reacción mediática en cadena a partir de las revelaciones de Aftergood. El mismo día 3 de enero, Poole publicó en el blog de CivicActions un artículo titulado 'Wikileaks - interesting to watch in 2007'. Inmediatamente después de estas revelaciones se produjeron los primeros contactos entre WikiLeaks y la prensa. La bandeja de correo electrónico de la organización se empezó a inundar de mensajes de periodistas interesados en informar sobre su actividad. Correos que fueron publicados en la página web de Cryptome, pocos días después, y que prueban el interés que WikiLeaks suscitó primero en periodistas de publicaciones especializadas como *Federal Times*, *Science Magazine* y *National Journal's Technology Daily*, a los que siguieron al día siguiente otros colegas de *New Scientist*, *Wired* o del periódico *The Washington Post*. Aquella atención prematura obligó a los miembros de WikiLeaks a "pensar de forma rápida y con cuidado cómo canalizarla", como se recoge en un correo filtrado, fechado el 4 de enero de 2007 (WikiLeaks Leak, 2007). El único nombre de sus miembros hecho público fue el de Hanna De Jong, la primera portavoz de WikiLeaks, la persona a la que se encomendó dar la cara en público por esta organización, en sus inicios, para garantizar el anonimato de Julian Asange y el de sus colaboradores más comprometidos en las filtraciones.

En sus primeras respuestas a la prensa, WikiLeaks ya hacía un llamamiento a la desobediencia civil:

> Favorecemos y defendemos el comportamiento ético en todas las circunstancias. No creemos en la obediencia incondicional a la autoridad en todas las circunstancias. Cada persona es el último árbitro de la justicia en su propia conciencia. Donde reina la injusticia y es consagrada por la ley, hay lugar para la desobediencia civil basada en principios. Donde el simple acto de distribución de información puede avergonzar a estructuras de poder autoritarias o exponer opresión o delitos graves, nosotros reconocemos un derecho, e incluso un deber, que hay que llevar a cabo. Tales denuncias implican a menudo un gran riesgo personal. Al igual que las leyes de protección de denunciantes en algunas jurisdicciones, este proyecto ofrece medios y la oportunidad de minimizar tales riesgos (WikiLeaks Leak, 2007).

Daniel Friedman, para *Federal Times*, y Aliya Sternstein, para *National Journal's Technology Daily*, fueron los primeros periodistas que publicaron una pieza informativa sobre WikiLeaks basada en fuentes primarias, el 4 de enero de 2007. Friedman tituló su artículo 'Web site aims to post government secrets'; Sternstein,

'Forthcoming Wiki Aims To Leak, Analyze Documents'. Por primera vez, se habló públicamente del uso que WikiLeaks hace de la tecnología criptográfica para asegurar el anonimato de sus filtradores, de la distribución y uso libre de su software, de su estrategia para contener y sortear probables ataques legales, y de sus potenciales fuentes de financiación para sostener el proyecto, principalmente "el Open Society Institute de la Soros Foundation, que promueve la democracia y los derechos humanos" (Friedman, 2007)[148].

Ese mismo día, varios profesionales de la comunicación se hicieron eco en sus blogs de estas revelaciones: Martin Stabe —periodista de datos de *Financial Times*— publicó 'A wiki for leaking secrets'; Dave Gilson —editor de la revista *Mother Jones*—, 'Whistleblowers get their own Wikipedia'; Hardy Haberman —escritor y cineasta conocido por ser un activista por los derechos de gays y lesbianas—, 'Wikileaks site will offer safe harbor for whistle blowers'; Beth Daley —investigadora de la organización independiente de Estados Unidos Project On Government Oversight, contra la corrupción gubernamental y por el fomento del gobierno transparente y ético—, 'Leaks go wiki'. Otra referencia fue publicada también en *Düsseldorf Blog* con el título 'Wikileaks - die gefährliche Abschaffung der Geheimnisse'.

A partir de estas primeras revelaciones, las publicaciones sobre WikiLeaks se sucedieron en cascada durante enero de 2007, tanto en medios especializados y alternativos —incluidos blogs y foros—, como en periódicos generalistas de todo el mundo, generando así el primer debate global sobre WikiLeaks y las filraciones masivas de secretos de Estado y corporativos.

A continuación mostramos, organizadas por fechas, las referencias más destacadas a WikiLeaks publicadas en medios heterogéneos, entre el 5 y el 31 de enero de 2007, y que son importantes para nosotros, como investigadores en comunicación, pues suponen la entrada de WikiLeaks en la esfera pública[149].

[148] Las citas tomadas de Friedman (2007) son traducciones propias del texto original, en inglés.
[149] Estas referencias las encontramos en búsquedas en Google para la palabra *wikileaks*, acotadas a enero de 2007, y en los registros del *wiki* de WikiLeaks, donde se conservan copias de algunos artículos borrados. El *wiki* está disponible en: https://wikileaks.org/wiki/Main_Page (último acceso: 20 de abril de 2015).

5 de enero:

'User generated smoking guns', por Quinn Norton en *Wired*; 'Is WikiLeaks.org the right idea for a whistleblowing website?', en *Spy Blog*.

6 de enero:

'Dokumente Befreien', por Jens Kubieziel en *Qbi's Weblog*.

7 de enero:

'Is Wikileaks A Good Idea?', en *Say Anything*; 'Gatekeeping is over', por Lotta Holmström en *Citizen Media Watch*; 'Il wikiventilatore? fa paura', por Vittorio Zambardino en *La Repubblica*; 'Tomorrow's Deep Throat: Wikileaks', por Goverup1 en *Daily Kos*.

9 de enero:

'WikiLeaks, il cane da guardia dei governi?', por Tommaso Poggiali en *Mytech.it*.

10 de enero:

'How to leak a secret and not get caught', por Paul Marks en *New Scientist*.

11 de enero:

'Wikileaks pone voz a la disidencia china en Internet', de la Agencia EFE en *El País*; 'Lanzarán sitio para filtrar documentos gubernamentales', por Jorge Martínez, en *Sociedad en Red*; 'Website wants to take whistleblowing online', en CBC News; 'Hush Hush Wikipedia', en *Canberra Times*; 'Opening up the rabbit hole', por Glasscastle en *Harvard's Dowbrigade Blog*; لك عل م حول ل ي مق راطيةل نشر مق ع ('Sitio para difundir la democracia en todo el mundo'), en *Al-Arab*.

12 de enero

'WikiLeaks desafía a la censura en Internet', de la Agencia EFE en *El Mundo*; 'Wikileaks spilled', por Quinn Norton en *Wired*; 'WikiLeaks, le partage Internet des dissidents', en *Marketing Etudiant*; 'Here's why Wikileaks is a horrible idea', por Paul McNamara en *Network World*; 'Listen up, whistleblowers!', por Lisa Lockwood en *Daily Kos*; לעשות עולם טוב יותר ('Hacer un mundo mejor'), en Notes.co.il; 'Wikileaks.org: сделай информацию свободной, организуй утечку данных!' ('WikiLeaks.org: ¡liberad la información, organizad la fuga de datos!'), en PGPRU.com.

13 de enero:

'Wikileaks ready to expose wrongs: Site offers anonymity to whistleblowers', por Chris Lackner en *Edmonton Journal*; 'Tattle in secret on new Web site', por Chris Lackner en *The Leader-Post*; 'Website's aim is to protect snitches: Now those who tell tales can do so in safety', por Chris Lackner en *Nanaimo Daily News*; 'Anonymity guaranteed on whistleblower website: Organizers say site will promote government changes; critics warn of credibility challenges', por Chris Lackner en *Times Colonist*; 'Website aims to protect identity of whistleblowers', por Chris Lackner en *Windsor Star*; 'Website aimed at providing forum for anonymous whistleblowers', por Chris Lackner en *The Vancouver Sun*; 'WikiLeaks website offers home for whistleblowers, no questions asked', por Torrance Mendez en *The West Australian*; 'WikiLeaks - bat na dyktaturę', por Edwina Bendyka en *Polityka*; 情報漏洩用Wiki「ウィキリークス」近日オープン予定 ('Un wiki de fugas de información abrirá próximamente') en Slashdot.jp.

14 de enero:

'Wikileaks: internetloket voor klokkenluiders', por Theo Dersjant en *De Nieuwe Reporter*; 'Wikifuites', por Ariane Krol en *Vigile.Québec*.

15 de enero:

'Freedom of information, the wiki way', por Elizabeth Williamson en *The Washington Post*; 'Wikileaks to serve as online Deep Throat', en United Press International; 'Wikileaks gives an online home to repressed dissidents', por Richard Koman en *ZDNet Government*; 'Courts, Injunctions, and WikiLeaks', por William McGeveran en *Harvard's Info/Law Blog*; 'Legger ut hemmelige dokumenter på nett', por Mats Bleikelia en *VG*; 'Wikileaks is a new tool for anonymous dissent', por Bill Boushka en *Bill on International Issues*; 'Wikileaks: More transparency for the policy common', por Dave Witzel en *Online Community Report*; 'Wikipedia inspira denúncia anônima na web', en *G1 - Globo*.

16 de enero:

'Serwis Wikileaks: przeciek ujawnisz dyskretnie', por Lukasz Partyka en *Gazeta.pl*; 'Wikileaks - the truth is in there… somewhere', en *bROkeN siMuLAcRA*; 'WikiLeaks, documenti segreti', en *La Stampa*; 異議份子出資／Wikileaks網站推動良知洩密運動 ('Disidentes colaboran con el sitio web WikiLeaks para promover un movimiento de filtraciones'), en *Liberty Times Net*.

17 de enero:

'Wikileaks: a site for exposure', por Scott Bradner en *Network World*; 'Dissidents take whistle-blowing global with leaking Web site', editorial en *Victoria Advocate*; 'Webseite für Staatsgeheimnisse', por Sonja Billhard en *Focus Online*.

18 de enero:

'Anonymous leaks in the Internet age', editorial en *Minnesota Daily*; 'Novo site ajuda anónimos a fazerem denuncias', en *Ciberia*; 'Powstaje internetowa platforma dla dysydentów', por Bartłomiej Ciszewski en *Money.pl*.

19 de enero:

'Site to serve as source for leaks', por Stephen Largen en *The Daily Tar Heel*.

20 de enero:

'Ich verrate Ihnen jetzt mal was! Wikis jüngster Ableger sammelt angebliche Geheimdokumente', por Britta Voss en *Süddeutsche Zeitung*; 'Website offers whistleblowers chance to go global', por Asher Moses en *The Sydney Morning Herald*.

21 de enero:

'Wikileaks, a másként gondolkodóknak', en *Sg.hu*; 'A wiki for whistle-blowers', por Tracy Samantha Schmidt en *Time*.

22 de enero:

'Complaining online becomes new social behaviour', por Shannon Proudfoot en *The Star Phoenix*; 'Bitch, bitch, bitch online: Got a complaint? There's a site for you as e-tattling grows, whether fair or not', por Shannon Proudfoot en *Windsor Star*; 'Complaining online popular', por Shannon Proudfoot en *The Leader-Post*; 'Are we a bunch of whiners?', por Shannon Proudfoot en *Kamloops Daily News*; 'Tattlers using the Internet as a weapon: Websites expose all: from leering men to sub-par service', por Shannon Proudfoot en *The Calgary Herald*; 'Online whining giving tattlers big audience', por Shannon Proudfoot en *The Halifax Daily News*; 'E-tattling becomes a new social trend', por Shannon Proudfoot en Nanaimo Daily News; 'Cyber leakers now have a place to go; Web site says goal is better government', por Rebecca Carr en *The Atlanta Journal-Constitution*; 'Whistleblowers now offered an outlet in private - the Wiki way', por Alexandra Sandels en *The Daily Star Egypt*; 'Wikileaks.org: kiszivárogtatási portál nemcsak újságíróknak', en *Transindex*.

23 de enero:

'Wikileaks: Collective Intelligence Agency?', en *Valeurdusage.net*; 'WikiLeaks.org: en wiki för hemliga dokument', por Lennart Frantzell en *Det Progressiva USA*; 'Summit held for internet code of conduct', por Steve Ragan en *Monsters & Critics*; 'Will Wikileaks keep anyone honest?', por m0j0 en *Musings of an anonymous geek*; دانس ه طرحم در ت رنتن یلا ('Documentos confidenciales en Internet'), por DonSaeid en *Tapesh.com*.

24 de enero:

'Anonymous is the new digital identity', por Roseleen Nzioka en *Flamme d'Afrique*; 'Bách khoa toàn thư trực tuyến về bí mật của các chính phủ', en *Dantri*; 'Un site internet pune în pericol documentele guvernamentale din întreaga lume', en *Adevarul*; 'Wikileaks and secrecy', por Stephen F. DeAngelis en *Enterra Insights*; 圧政を敷く国々"を告発するWikileaks ('WikiLeaks, para denunciar las tiranías en el mundo'), en *ITmedia*.

25 de enero:

'Geheimnisverrat bei Wikileaks', por Hendrik Werner en *Die Welt*.

27 de enero:

'The week on the web: The truth is out there… maybe', por Rhys Blakely en *The Times*.

29 de enero:

'Terror of the silent whistler', por Billy Simpson en *Belfast Telegraph*.

30 de enero:

'Revolution via nettet: ny central for afsloerende dokumenter', por Peter Wivel en *Politiken*; 'Wikileaks.org: la «garganta profunda» de la Red', por Marta Peirano en *Eroski Consumer*.

Identificar estas primeras referencias públicas a WikiLeaks nos facilita no sólo conocer su génesis, sino también reconocer en los blogs, foros y medios especializados en línea la principal fuente de energía cinética en la diseminación de WikiLeaks en su origen en el ciberespacio. Pero también permite comparar la narrativa primitiva sobre WikiLeaks con la actual y evaluar la dimensión global, políglota y polifónica de su irrupción en la esfera pública.

Estas primeras publicaciones se vieron además alimentadas con una segunda filtración de información privada de WikiLeaks y la primera conspiración contra esta organización, que fue acusada de ser un instrumento de la CIA. El 7 de enero de 2007, John Young publicó en la página web de Cryptome la primera serie de los correos de la lista de WikiLeaks; dos días después, publicó una segunda serie. Esto fue una paradoja para una organización que se presentaba como segura y que protegía a sus miembros. Sólo la decisión de Young de no revelar la identidad de los participantes en aquella lista de correo —la mayoría de nombres y direcciones de correo electrónico fueron borrados por Young, en un acto de coherencia ética— permitió a los individuos más comprometidos en la revelación de secretos seguir manteniéndose en el anonimato.

Pero las filtraciones de Young no sólo expusieron cómo se estaba gestando la mayor maquinaria de filtraciones de información secreta del mundo, también elevaron el debate y la controversia sobre WikiLeaks, suscitando las primeras críticas a esta organización. Young acusó a WikiLeaks de ser una herramienta de una sofisticada operación encubierta de la CIA para desinformar a la población mundial. Sin embargo, el cofundador de Cryptome nunca presentó ninguna prueba de ello; su acusación se basó en meras especulaciones que acabó él mismo por desmentir, aunque siguieron inspirando teorías conspirativas como la vertida por Daniel Estulin en su libro *Desmontando a WikiLeaks* (2011), donde especula con que esta organización es un artificio creado por la CIA para justificar el control de Internet.

Pese a esta explosiva irrupción de WikiLeaks en la esfera pública, esta organización no tuvo un impacto significativo en la opinión pública hasta el año 2010, cuando decidió aliarse con algunos de los más importantes medios de comunicación del mundo para dar a conocer los documentos que poseía sobre el Gobierno de Estados Unidos.

En sus primeros tres años de actividad, WikiLeaks hizo sustanciales revelaciones de información secreta; por ejemplo: un informe sobre el expresidente keniano Daniel Arap Moi que desveló cómo saqueó su país al apropiarse de unos mil quinientos millones de euros; la publicación del manual de procedimiento militar en el Campamento Delta de la base de Guantánamo de Estados Unidos; información confidencial sobre el banco de inversión suizo Julius Bär; la difusión de fotografías y extractos de correos electrónicos personales de la gobernadora ultraderechista de Alaska y candidata republicana a la vicepresidencia de Estados Unidos en el año 2008, Sarah Palin; o más de tres mil mensajes de correo electrónicos intercambiados por algunos de los climatólogos más influyentes del mundo. Sin embargo, el impacto de WikiLeaks en la opinión pública fue muy limitado en sus primeros tres años de actividad. "Como sus comunicaciones internas dejan claro, Assange estaba perplejo y consternado por la indiferencia del mundo a sus filtraciones" (Manne, 2011). Todo cambió en 2010, cuando Assange decidió dar un giro de 180 grados a su estrategia.

IV.5.3.2. 2010. Cambio de estrategia: geoposicionamiento del mensaje a través de cinco medios globales e influyentes en Occidente

Alan Rusbridger, editor de *The Guardian*, resume 2010 como el año en el que Julian Assange se volvió viral al orquestar la mayor filtración de documentos secretos de la historia. "La única diferencia era que, esta vez, la vergüenza no iba para una pobre nación de África oriental, sino para el país más poderoso de la Tierra" (Leigh y Harding, 2011: 16-17).

El primer gran impacto mundial de WikiLeaks en los medios de comunicación, la opinión pública y la política se produjo el 5 de abril de 2010, con la publicación del dramático vídeo grabado el 12 de julio de 2007 desde un helicóptero Apache estadounidense en Irak, en el que se ve cómo soldados estadounidenses acribillan al reportero de la agencia de noticias Reuters Namir Noor-Eldeen, a su ayudante y a diez

civiles más. Para difundirlo, WikiLeaks lo tituló *Collateral Murder*, creó *ex profeso* un sitio web[150] y eligió estratégicamente el National Press Club de Washington para su presentación mundial en conferencia de prensa. La cadena árabe Al Jazeera y el canal ruso RT fueron los primeros que le dieron una amplia atención, además de la agencia Reuters, obviamente por su implicación en aquella operación de los soldados estadounidenses en la que murió uno de sus reporteros y su colaborador. A estos medios les siguieron los periódicos *The Washington Post*, *The New York Times*, *The Guardian* y *El Mundo*, y las cadenas de televisión BBC y CNN, entre otros medios.

El 21 de junio de 2010, Assange se reunió en el hotel Leopold de Bruselas con Nick Davies, periodista de *The Guardian*. Assange disponía de cientos de miles de documentos secretos filtrados por el soldado Bradley E. Manning, un imberbe analista de inteligencia del Ejército de Estados Unidos destinado en Irak y detenido allí el 26 de mayo de 2010, acusado de sustraer documentos clasificados de las redes secretas del Pentágono y de entregárselos a WikiLeaks. A Manning se le artribuyó la responsabilidad de las filtraciones del vídeo del caso *Collateral Murder* y de cientos de miles de documentos sobre las guerras de Irak y Afganistán y de la diplomacia estadounidense. Manning era un analista de inteligencia del Ejército de Estados Unidos con acceso a SIPRNet, el protocolo secreto de redes de enrutado de Internet (Secret Internet Protocol Router Network), la versión secreta de la Red que opera el Departamento de Defensa de Estados Unidos. Manning fue acusado de robar y revelar información clasificada usando un simple CD regrabable, rotulado con el nombre de la cantante Lady Gaga para no levantar sospechas. Las autoridades estadounidenses le atribuyeron la filtración a WikiLeaks de cientos de miles de documentos de Estados Unidos: 391.831 de la guerra de Irak, 91.731 de la guerra de Afganistán, 251.287 de la diplomacia de Estados Unidos, 779 de presos en la base militar de Guantánamo o el vídeo de *Collateral Murder*, entre otros.

Assange quería publicar en bruto y masivamente en la página web de WikiLeaks aquel enorme alijo de documentos secretos, pero Nick Davies lo convenció para que lo hiciera a través de una alianza de medios importantes. Tras cerrar el acuerdo con *The Guardian*, la dirección del periódico británico contactó al otro lado del Atlántico con el entonces editor de *The New York Times*, Bill Keller, para que se sumara a este acuerdo

[150] Página web de *Collateral Murder*: http://collateralmurder.com.

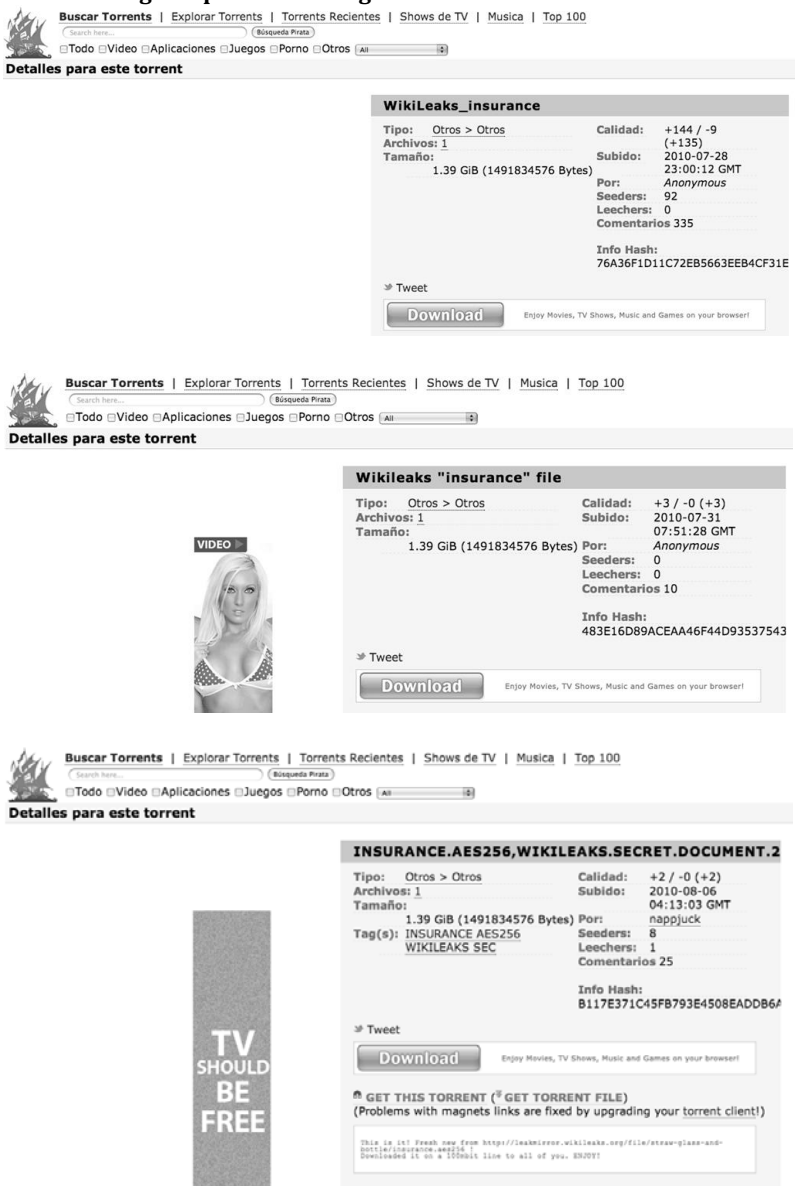
con WikiLeaks. El propio Julian Assange explica en una entrevista en el documental *WikiLeaks: Secrets and Lies* la nueva estrategia que había decidido emprender: "Necesitábamos tener un socio estadounidense que maximizara la protección de la fuente o fuentes, que seguramente eran estadounidenses" (Assange, en Forbes, 2011). A los periódicos británico y estadounidense se les sumó el alemán *Der Spiegel*. Así, la sede de *The Guardian* en Londres se convirtió en el cuartel general de esta operación. El tema más recurrido y más conflictivo en aquellas reuniones fue la protección de las identidades de las personas que aparecían en aquellos documentos secretos, por motivos de seguridad personal. Mientras los periodistas se aferraban a sus principios éticos y deontológicos tradicionales para proteger a esas personas, la ética hacker de Julian Assange le hacía colocarse en una posición radicalmente opuesta: la información debía ser liberada en bruto, sin suprimir datos, sin editar el contenido de los documentos, porque para él eso era lo correcto. La información, toda la información, debía estar al alcance de todo el mundo. Sin embargo, Assange sí era muy celoso en la protección de las fuentes que le filtraban información.

El 25 de julio de 2010 tuvo lugar la primera gran filtración masiva de documentos de WikiLeaks. Eran archivos sobre la guerra global contra el terrorismo que habían emprendido Estados Unidos y sus aliados tras los atentados del 11 de septiembre de 2001. Assange decidió empezar a trabajar conjuntamente y de manera estrecha con algunos de los periódicos más importantes de Occidente: WikiLeaks filtró a *The Guardian* (británico), *The New York Times* (estadounidense) y *Der Spiegel* (alemán) casi 92.000 documentos sobre la guerra de Afganistán referidos al periodo comprendido entre los años 2004 y 2009. Esta filtración fue bautizada como *Afghan War Diary*, o también *Afghanistan War Logs*, pero también se conocieron popularmente como *Los Papeles de Afganistán*, estableciendo un manifiesto paralelismo con *Los Papeles del Pentágono* que en 1971 filtró Daniel Ellsberg a *The New York Times*.

A raíz de la condena expresada por el Gobierno de Estados Unidos por esta filtración de documentos secretos, WikiLeaks añadió en su página web de los *Diarios de Guerra de Afganistán* el misterioso archivo encriptado *insurance.aes256*, de 1,39 gigabytes. El bautizado como *Insurance File* se codificó usando el algoritmo AES 256 (Advanced Encryption Standard) y se ofreció también en un archivo *torrent* en páginas

web de descarga como The Pirate Bay[151], a finales de julio y primeros días de agosto del año 2010. Se ha especulado en distintos sitios de Internet con que se trataría de una filtración cuya contraseña sería liberada en caso de que WikiLeaks sufriese algún ataque grave que provocase que la organización quedara incapacitada. También se ha dicho que se trataría de una suerte de seguro de vida de Assange.

Ilustración 20: Páginas para la descarga del archivo *insurance.aes256*.



Fuente: capturas propias tomadas de las páginas de The Pirate Bay donde se aloja el archivo *insurance.aes256*.

151 Enlaces para la descarga del archivo en The Pirate Bay:
http://thepiratebay.se/torrent/5728614
http://thepiratebay.se/torrent/5741985
https://thepiratebay.se/torrent/5723136.

La siguiente gran filtración fue la que se produjo el 22 de octubre de 2010 sobre la guerra de Irak, con el título *Irak War Logs*. Los *Diarios de Guerra de Irak* se convirtieron en la mayor publicación instantánea de material clasificado en la historia: 391.832 documentos filtrados del Pentágono sobre el conflicto en Irak entre los años 2004 y 2009. WikiLeaks los expuso en su sitio web y llegó, otra vez, a un acuerdo de colaboración con los tres periódicos anteriormente citados, más *Le Monde* (francés), la cadena Al Jazeera (mundo árabe) y el Bureau of Investigative Journalism (organización británica sin ánimo de lucro).

La segunda mayor filtración hasta ese momento, y la de mayor impacto mediático y político, se produjo el 28 de noviembre de 2010, cuando WikiLeaks reveló que tenía en su poder 251.287 cables y comunicaciones entre el Departamento de Estado de Estados Unidos y sus embajadas por todo el mundo, de los cuales más de cien mil estaban clasificados. Aunque oficialmente fue denominada *United States Diplomatic Cables Leak*, esta operación se hizo popular con el nombre *Cablegate*, otra evidente comparación histórica, en este caso con el que era considerado el mayor hito del periodismo moderno: el caso *Watergate*. Para difundir estas filtraciones, WikiLeaks dio un nuevo giro a su estrategia y llegó a un acuerdo de exclusividad con *The New York Times*, *The Guardian*, *Der Spiegel*, *Le Monde* y, por primera vez, el español *El País*, para que sus periodistas seleccionasen, trabajasen y publicasen los cables diplomáticos según sus propios criterios editoriales. Esta colaboración con algunos de los más influyentes medios en Occidente respondió a una estrategia de geoposicionamiento del mensaje para impactar de manera más efectiva en la opinión pública. "Trabajando a través de fronteras nacionales [WikiLeaks] aseguró que las historias serían impulsadas por intereses locales, pero con consecuencias internacionales" (Uricchio, 2014: 2569). Así describe WikiLeaks su estrategia:

> […] WikiLeaks ha estado liberando cables diplomáticos de Estados Unidos de acuerdo con un plan cuidadosamente trazado para estimular cambios profundos. El método WikiLeaks implica un procedimiento sofisticado de agrupamiento de cables diplomáticos filtrados de Estados Unidos en grupos nacionales o temas […], proporcionados a las organizaciones que estuvieron de acuerdo en realizar la investigación a cambio de exclusividad limitada en el tiempo. Como parte del acuerdo con WikiLeaks, estos grupos, usando su conocimiento local, eliminan los nombres de las personas que denuncian actos injustos a las embajadas de Estados Unidos y proporcionan los resultados a WikiLeaks. WikiLeaks publica a continuación, de forma simultánea con sus socios, estos cables con revelaciones políticamente explosivas (WikiLeaks, 2011a).

Esta coalición mediática supuso un punto de inflexión en la estrategia comunicativa de WikiLeaks, que legitimó así el papel de *gatekeepers* de los medios y su modelo de selección, verificación, edición y jerarquización de la información, contradiciendo así los principios que habían regido la actividad de WikiLeaks como organización adscrita a la ética hacker: acceso libre y sin restricciones a la información y a cualquier tecnología intelectual que enseñe algo sobre cómo funciona el mundo, descentralización, desconfianza en las estructuras de poder establecidas y confianza en los ordenadores como herramientas para mejorar nuestras vidas; lucha contra la aliencación del ser humano y búsqueda de la verdad (Levy, 1984).

Como explica Charlie Beckett —director fundador de POLIS, *think tank* en el departamento Media and Communications de la London School of Economic—, en una entrevista en *Editors Weblog*, WikiLeaks eligió a las grandes publicaciones tradicionales porque "querían el acceso a las audiencias", pero "esto significaba que tenían que editar lo que estaban haciendo, compartir información" (Vinter, 2011).

El éxito de Wikileaks "depende necesariamente de la capacidad para aprovechar la publicidad proporcionada por los medios de comunicación convencionales" (Andrejevic, 2014: 2626)[152], que aún gozan de una posición dominante.

> Un medio alternativo como WikiLeaks es menos probable que sea reconocido, leído y dominado por ciudadanos comunes. No es ninguna sorpresa, sino más bien un reflejo de la economía política de los medios de comunicación en el capitalismo (Fuchs, 2014: 2727)[153].

A la vez, estos grandes medios de información confirieron a WikiLeaks credibilidad y legitimidad (Maurer, 2011) y posibilitaron que las filtraciones fuesen publicadas como "actos periodísticos responsables" (Uricchio, 2014: 2569). Ésta es una tesis en la que coinciden diversos analistas.

> WikiLeaks aún depende de los grandes medios de comunicación —generalmente impresos— para conferir legitimidad periodística al flujo de documentos de los que dispone. Necesita del referéndum y de la purificación formal de la verificación periodística (Saad Corrêa, 2011: 217).

Como contrapartida, WikiLeaks ofreció a estos medios una ventaja competitiva en sus mercados: la exclusividad, un salvavidas en un momento crítico para la prensa,

[152] Las citas tomadas de Andrejevic (2014) son traducciones propias.
[153] Traducción propia.

que vive su mayor crisis de credibilidad y de negocio. El sitio web de *The Guardian*, por ejemplo, registró 4,1 millones de usuarios únicos el día de la liberación del *Cablegate* —el número más alto de su historia— y entre el 28 de noviembre —día de la liberación de los cables diplomáticos— y el 14 de diciembre de 2010, un total de 9,4 millones de usuarios consultaron los contenidos dedicados a WikiLeaks en el sitio web de *The Guardian*. Alrededor del 43 por ciento de todo el tráfico web procedía de Estados Unidos (Leigh y Harding, 2011: 225).

Así, WikiLeaks era validado por la prensa, esta recuperaba el estatus, prestigio y confianza perdido por dejadez de sus funciones (Andrejevic, 2014: 2624), y ambas partes se regalaban credibilidad, originando una situación de *win-win* para ambas partes (Pacheco, 2011: 32).

Además, al elegir a la prensa tradicional, Assange aseguró algunas protecciones legales para WikiLeaks (Maurer, 2011).

> Él y sus compañeros tecnológos ya habían logrado uno de sus objetivos: habían hecho que WikiLeaks resultara prácticamente indestructible y, por tanto, quedara fuera del alcance de cualquier ataque legal o cibernético desde cualquier otra jurisdicción o fuente. Abogados que cobraban sumas exorbitantes de dinero para proteger la reputación de sus adinerados clientes y corporaciones admitieron —con voces embargadas de una mezcla de frustración y admiración— que WikiLeaks era la única editorial del mundo que eran incapaces de amordazar. Eso era muy malo para el negocio. (Leigh y Harding, 2011: 17).

Assange, como buen estratega, se parapetó tras los periodistas de estos cinco medios, intentando asegurarse para él y WikiLeaks las protecciones legales que les son *propias* a los periodistas y a las empresas informativas, de tal modo que cualquier acción contra el fundador de WikiLeaks o su organización por sus filtraciones supondría un ataque directo a la libertad de prensa de cinco de los medios más influyentes del mundo. Así lo explican Leigh y Harding:

> A principios de 2011 había síntomas de frustración creciente entre las autoridades gubernamentales de EE.UU. al registrar el mundo en busca de pruebas que pudieran utilizar contra él, incluida la citación de sus cuentas en tuiter [*sic*]. Hubo también, entre los magistrados más serenos, el reconocimiento de que resultaría prácticamente imposible procesar a Assange por el acto de publicación de los diarios de guerra o de los cables del Departamento de Estado sin también llevarse por delante a cinco directores de periódicos. Eso sería el caso periodístico del siglo (Leigh y Harding, 2011: 25).

Al mismo tiempo, los periódicos colaboradores aceptaron los compromisos a los que pudiera llegar *The New York Times* con el Departamento de Estado de Estados Unidos, que hizo también funciones de *gatekeeper*. "Ellos eligen qué debe publicarse y cómo bajo la asesoría del Departamento de Estado, según señala un editorial de *The New York Times*" (Villeda Saldaña, 2011: 69). Así, el proceso de liberación de los cables no fue un ejercicio de periodismo libre, sino más bien una nueva escenificación de la sumisión de los medios tradicionales a los imperativos del Estado-nación y sus estructuras de control, ya que el *Times* "informó al Gobierno de los Estados Unidos de todos y cada uno los cables que iban a publicar" (Assage, en Hastings, 2012: 48).

El 28 de noviembre de 2010, *El País* presentó la publicación del *Cablegate* en un artículo titulado 'La mayor filtración de la historia deja al descubierto los secretos de la política exterior de EE UU'. En este amplísimo artículo hay que irse al párrafo 25 para encontrar, como aguja en un pajar, la mención a este acuerdo alcanzado por The New York Times con las autoridades estadounidenses para poner filtros a las revelaciones.

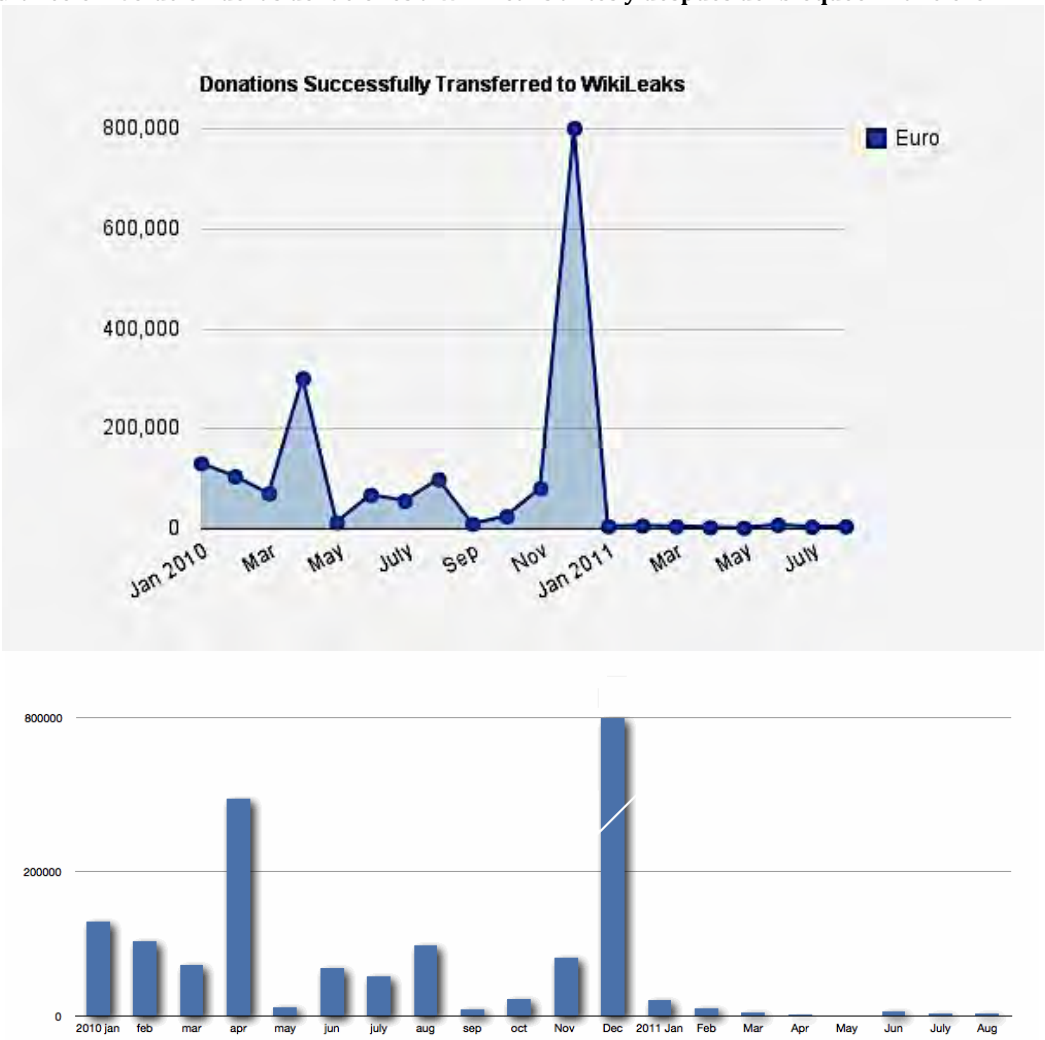
> Entre otras precauciones, se ha decidido aceptar los compromisos a los que *The New York Times* llegue con el Departamento de Estado para evitar la difusión de determinados documentos (Jiménez y Caño, 2010).

Este pacto pasó desapercibido para la opinión pública y para algunos analistas del fenómeno WikiLeaks, a pesar de la trascendencia periodística y política que supone la intervención del Departamento de Estado como órgano censor o supervisor.

A partir de la publicación de los cables diplomáticos de Estados Unidos, todo se precipitó en apenas medio mes. El 3 de diciembre de 2010, se puso en marcha en Estados Unidos la SHIELD Act (Securing Human Intelligence and Enforcing Lawful Dissemination), una enmienda a la Ley de Espionaje de 1917 (Espionage Act) que ya prohíbe la divulgación pública de información clasificada de actividades de inteligencia de Estados Unidos. Esta reforma de ley, diseñada *ex profeso* para el caso WikiLeaks, buscaba ampliar la prohibición y tipificar como delito federal cualquier publicación de información relativa a la identidad de cualquier fuente clasificada de inteligencia o a actividades de inteligencia humana de Estados Unidos o de otro país extranjero, si tal publicación es perjudicial para los intereses de Estados Unidos.

Además, grandes empresas de las que WikiLeaks dependía económica y tecnológicamente para su supervivencia —Paypal, Mastercard, Visa, Bank of America, Western Union, PostFinance, Amazon, EveryDNS— boicotearon con un bloqueo a la organización, presionadas por el discurso beligerante del Gobierno de Estados Unidos y de políticos de este país contra WikiLeaks, destruyendo el 95 por ciento de sus ingresos (WikiLeaks, 2011b), lo cual ha sido interpretado como un ataque al derecho de libertad de expresión de WikiLeaks (Daly, 2014: 2694).

Gráfico 6: Evolución de las donaciones a WikiLeaks antes y después del bloqueo financiero.



Fuente: https://www.wikileaks.org/Banking-Blockade.html.

Julian Assange fue detenido por la Policía londinense el 7 de diciembre por los cargos de presunta violación y abusos sexuales que pesaban sobre él en Suecia desde agosto de 2010, lo cual abría las puertas a una futurible extradición a Estados Unidos

para que fuese juzgado allí por revelación de secretos de Estado. El grupo hacktivista Anonymous inició entonces una campaña en el ciberespacio para vengar a Julian Assange, bloqueando las páginas web de la Fiscalía de Suecia, Mastercard, Visa y PayPal. La detención de Assange fue el punto de intersección entre WikiLeaks y Anonymous, dos entidades hacktivistas que, aunque no pueden ser más diferentes en sus mecanismos organizativos y operativos (Coleman, 2014: 88), convergen por sus ideales y fines.

El fenómeno ya era imparable. El universo WikiLeaks se expandía viralmente a la vez que los medios de comunicación de masas descubrían el potencial de la colaboración, de las redes electrónicas y de la alta tecnología, combinadas. Es lo más cerca que han estado de la cultura hacker.

> Una de las lecciones del proyecto WikiLeaks es que ha demostrado las posibilidades de la colaboración. Es difícil pensar en un ejemplo comparable de colaboración entre organizaciones de noticias similar a como han trabajado el *Guardian*, *The New York Times*, *Der Spiegel*, *Le Monde* y *El País* en el proyecto WikiLeaks (Leigh y Harding, 2011: 25).

IV.5.3.3. 2011-2012: ruptura de relaciones y nuevas filtraciones y alianzas

A lo largo del año 2011 se fueron escenificando los desencuentros entre Jullian Assange y los medios de información que había seleccionado como colaboradores necesarios para difundir los contenidos de los cables diplomáticos y lograr, a través de ellos, sus objetivos: máximo impacto político y publicidad para WikiLeaks. Durante ese año y a principios de 2012 se produjeron tres grandes filtraciones. Y todo ello, en medio de la trama judicial en la que se vio envuelto el editor de WikiLeaks, la orden de extradición a Suecia, la guerra dialéctica a escala mundial entre defensores y detractores de Assange, y la ascendente popularidad del personaje, con la publicación y preparación de un buen número de documentales, películas, libros, videojuegos, etc. Nuevos escenarios para una historia que no dejó de ser aderezada con más revelaciones de documentos secretos, aunque con menor impacto público, y la polémica publicación por parte de WikiLeaks de la totalidad de los cables diplomáticos a su disposición, sin ocultar la identidad de las fuentes; un hecho que patentizó el creciente desencuentro con los medios que habían colaborado en el *Cablegate*:

> […] el matrimonio de conveniencia de los medios tradicionales con WikiLeaks o de ésta con ellos terminó en septiembre de 2011 cuando WikiLeaks decidió publicar íntegramente los cables diplomáticos sin que los periodistas tradicionales filtraran previamente la información (Elías, 2011: 7).

Para tomar esta espinosa decisión, WikiLeaks decidió compartir esta responsabilidad con sus seguidores, a los que invitó el 1 de septiembre de 2011, a través de Twitter, a votar si era conveniente o no que la organización publicara en su sitio web todos los cables diplomáticos en bruto que tenía en su posesión, sin tachar nada, sin pasar por el filtro de ningún medio de información tradicional.

Ilustración 21: WikiLeaks [wikileaks]. (2011, Sep 01). Global vote: should WikiLeaks release all US cables in searchable form? tweet #WLVoteYes or #WLVoteNo Why: http://t.co/GGON8cd [Tweet]. Recuperado de https://twitter.com/wikileaks/status/109068142260649984

Al día siguiente, WikiLeaks anunció en Twitter la liberación de todos los cables en su página web.

Ilustración 22: WikiLeaks [wikileaks]. (2011, Sep 02). Shining a light on 45 years of US "diplomacy", it is time to open the archives forever. http://t.co/ViHlu8o [Tweet]. Recuperado de https://twitter.com/wikileaks/status/109435223200104448

Esta decisión provocó las críticas de los cinco medios que se habían coaligado en el caso *Cablegate*. En una nota conjunta publicada el 2 de septiembre, *The New York Times*, *The Guardian*, *Der Spiegel*, *Le Monde* y *El País* lamentaron y condenaron la publicación de la totalidad de los 251.287 cables sin ocultar la identidad de las fuentes, al considerar que "la revelación de la identidad de los informantes podría poner en peligro a las citadas fuentes" ('WikiLeaks anuncia la publicación de todos sus cables diplomáticos sin proteger a sus fuentes', 2011).

Ilustración 23: *The New York Times, The Guardian, Der Spiegel, Le Monde y El País* condenan la publicación en bruto de todos los cables diplomáticos de Estados Unidos en poder de WikiLeaks.


EL PAÍS.com | Internacional

Sábado, 26/11/2011, 20:29 h EL PAIS en KIOSKO y más

Inicio | Internacional | Política | España | Deportes | Economía | Tecnología | Cultura | Gente y TV | Sociedad | Opinión | Blogs | SModa | In English

América Latina | Europa | Estados Unidos | Oriente Próximo | Corresponsales

ELPAIS.com > Internacional

Wikileaks anuncia la publicación de todos sus cables diplomáticos sin proteger a sus fuentes

EL PAÍS, 'The New York Times', 'The Guardian', 'Der Spiegel' y 'Le Monde' lamentan la decisión de la organización de Assange

EL PAIS - Madrid - 02/09/2011

Vota ☆☆☆☆☆ | Resultado ★★★★½ 206 votos | Twittear 315 | Recomendar 694

Consulta el especial de Wikileaks

Wikileaks ha anunciado la publicación de la totalidad de los 250.000 cables diplomáticos a su disposición sin ocultar la identidad de las fuentes. Cinco medios de comunicación internacionales -*The New York Times, The Guardian, Le Monde, Der Spiegel* y El PAÍS- condenan la decisión de Wikileaks de publicar estos cables por considerar que la revelación de la identidad de los informantes podría poner en peligro a las citadas fuentes. Reporteros sin Fronteras ha decidido retirar temporalmente su apoyo a la organización tras conocer las noticias de la publicación.

Fuente: captura de pantalla propia tomada de la edición digital de *El País* del 2 de septiembre de 2011. http://internacional.elpais.com/internacional/2011/09/02/actualidad/1314914403_850215.html (última consulta: 30 de noviembre de 2011).

Una vez que la relación entre WikiLeaks y estos medios se rompió y los cables fueron liberados en masa por esta organización, el escenario cambió considerablemente, "negándosele a WikiLeaks la protección de la prensa, aliviando a ésta y al público de la tensión dramática de esperar el próximo episodio, y poniendo el foco central en la cuestión más amplia de la fiabilidad del narrador" (Uricchio, 2014: 2570).

En la guerra dialéctica entre Julian Assange y los periodistas de los medios excolaboradores de WikiLeaks, el hacker australiano ha sido especialmente beligerante con *The New York Times*, periódico al que acusa de haber iniciado el conflicto entre las partes y de ponerse al servicio de los intereses del Gobierno de Estados Unidos:

> El *Times* abrió fuego; nos abandonó cuando la administración estadounidense empezó a molestarse. Al hacerlo, también se abandonó a sí mismo y a todos los periodistas que trabajan en el ámbito de la seguridad nacional en los Estados Unidos. Lo que le preocupaba al *Times* era verse involucrado en una investigación gubernamental […] Nos dijeron que nunca debíamos referirnos al periódico como un socio, ese fue su consejo legal (Assange, en Hastings, 2012: 48).

Este desencuentro entre WikiLeaks y los periodistas alcanzó su cenit el 28 de noviembre de 2011, en una intervención de Assange, vía Skype, en el Global Editors Network celebrado en Hong Kong. El fundador de WikiLeaks acusó a los editores de las empresas informativas de estar "corrompidos por el poder" y a la mayoría de periodistas, de entrar en la profesión para "trepar por la escalera del poder para asociarse con el poder" (Bartlett, 2011). Una vez desprestigiados los grandes medios tradicionales y enfatizada su "crisis de legitimidad" –la que habían recuperado gracias a WikiLeaks–, Assange contrapuso la labor de éstos con la "virtud moral" de WikiLeaks que obliga a gobiernos y corporaciones a rendir cuentas ante la sociedad. Assange daba así el último giro a esta historia, colocando a los medios tradicionales como cómplices de los villanos, a WikiLeaks como nuevo guardián de la democracia y la libertad, y a él, como héroe protagonista de esta historia (McAthy, 2011).

Ilustración 24: Assange acusa a los ediores de medios de estar corrompidos por el poder.

Fuente: captura de pantalla propia de la edición del 28 de noviembre de 2011 de http://www.journalism.co.uk/news/assange-accuses-editors-of-being-corrupted-by-power/s2/a546922/ (último acceso: 28 de noviembre de 2011).

Para cuando las relaciones de WikiLeaks y los grandes medios de información globales de Occidente se rompieron, Julian Assange ya había conseguido el principal objetivo de su organización: el máximo impacto mediático y político. A partir de entonces, las cosas cambiaron, como explica Nick Davies, de *The Guardian*, en el documental *WikiLeaks: Secrets and Lies*. El hecho de no haber modificado los documentos de la guerra de Afganistán para proteger las identidades de militares, fuentes y otros actores implicados directamente en el conflicto armado, y la petición de extradición que pesaba sobre Assange en Suecia por presuntos abusos sexuales a dos mujeres, además de la propia personalidad y actitud desafiante del fundador de WikiLeaks, habrían hecho perder autoridad moral, impacto político y credibilidad a Assange y WikiLeaks, en opinión de Davies (Forbes, 2011).

Las filtraciones de WikiLeaks de documentos secretos continuaron durante los años 2011 y 2012. El 27 abril de 2011, WikiLeaks comenzó a publicar 779 informes secretos del Pentágono, fechados entre 2002 y 2009, relacionados con los abusos a prisioneros detenidos en el campamento de detención de Guantánamo. Estos informes, conocidos como los *Guantanamo Bay Files*, demostraban que el 60 por ciento de los prisioneros fue conducido a esta base militar estadounidense sin ser una amenaza "probable" y que allí se imponía un sistema penal y policial sin garantías para los reos[154].

El 1 de diciembre de 2011, WikiLeaks inició la publicación de los *Spy Files*[155], 287 documentos que contienen información sobre las actividades de compañías de seguridad, vigilancia y espionaje de veinticinco países. Los documentos fueron sacados a la luz con la colaboración de Bugged Planet (proyecto colaborativo y público contra la vigilancia global, creado por Andy Müller-Maguhn, del Chaos Computer Club)[156] y Privacy International (ONG británica que defiende el derecho a la privacidad de los individuos)[157], así como de organizaciones mediáticas de seis países: *The Washington Post* (Estados Unidos), *L'Espresso* y *La Repubblica* (Italia), *The Hindu* (India), OWNI (Francia), ARD (Alemania) y el Bureau of Investigative Journalism (Reino Unido). La intención de WikiLeaks era denunciar el funcionamiento de la tecnología de vigilancia y espionaje que gobiernos y corporaciones pueden adquirir y usar para espiar a individuos

154 En: https://wikileaks.org/gitmo/ (último acceso: 15 de julio de 2015).
155 En: http://wikileaks.org/the-spyfiles.html (último acceso: 15 de julio de 2015).
156 En: http://buggedplanet.info/ (último acceso: 17 de julio de 2015).
157 En: https://www.privacyinternational.org/ (último acceso: 17 de julio de 2015).

o poblaciones enteras. Este caso fue el antecedente de la extraordinaria revelación que luego hizo el analista Edward Snowden en 2013, al destapar el sistema de vigilancia global y masiva del Gobierno de Estados Unidos y de algunos de sus aliados.

El 27 de febrero de 2012, WikiLeaks comenzó otra colaboración con medios de comunicación para la publicación de cinco millones y medio de correos electrónicos de la empresa de inteligencia global Strategic Forecasting, Inc., más conocida como Stratfor, con sede central en el estado de Texas. La fitración masiva fue atribuida a una incursión de miembros de Anonymous en el sitio web de Stratfor, (Ball, 2012). En concreto, sus autores fueron hackers de AntiSec —contracción de Anti-Security— facción surgida en verano de 2011, en plena fragmentación de Anonymous en un archipiélago de islas hackers (Coleman, 2014: 283). Aquélla fue la acción más memorable de AntiSec.

Bautizados como *The Global Intelligence Files*[158], estos documentos, fechados entre julio de 2004 y finales de diciembre de 2011, revelan el funcionamiento y técnicas utilizadas por Stratfor, y las relaciones de esta compañía privada de espionaje con sus clientes, entre los que se encuentran la CIA, ministerios de Defensa y Exteriores, embajadas y compañías multinacionales. Deterioradas las relaciones con los cinco grandes medios colaboradores en el *Cablegate*, WikiLeaks recurrió para esta filtración masiva —la mayor, por su volumen— a veintinueve medios de todo el mundo, más repartidos geográficamente, culturalmente más heterogéneos y de naturaleza diversa, pero, en general, menos populares e influyentes a nivel mundial:

- *ABC Color* – Paraguay.
- *Al Akhbar* – Líbano.
- *Al Masry Al Youm* – Egipto.
- *Asia Sentinel* - Hong Kong.
- *Bivol* – Bulgaria.
- *Carta Capital* – Brasil.
- *CIPER* – Chile.
- *Dawn Media* – Pakistán.
- *L'Espresso* – Italia.
- *La Repubblica* – Italia.
- *La Jornada* – México.
- *La Nación* – Costa Rica.
- *Malaysia Today* – Malasia.

[158] Véase http://wikileaks.org/the-gifiles.html (último acceso: 15 de julio de 2015).

- *McClatchy* – Estados Unidos.
- *Nawaat* – Túnez.
- *NDR/ARD* – Alemania.
- *Owni* – Francia.
- *Pagina 12* – Argentina.
- *Plaza Pública* – Guatemala.
- *Pública* – Brasil.
- *Público* – España.
- *Rolling Stone* – Estados Unidos.
- *Russia Reporter* – Rusia.
- *Sunday Star-Times* – Nueva Zelanda.
- *Ta Nea* – Grecia.
- *Taraf* – Turquía.
- *The Hindu* – India.
- The Yes Men[159] – Global.

Tras varias semanas de publicaciones, WikiLeaks decidió ampliar su red de socios mediante un sistema de invitaciones personales y confidenciales a periodistas, investigadores académicos y activistas, seleccionados por esta organización para diversificar el trabajo y amplificar el eco de las filtraciones en tres campos estratégicos: los medios de comunicación de masas, la Academia y las organizaciones no gubernamentales de derechos humanos, en cualquier idioma y con distintos radios de influencia. Este sustancial giro en su estrategia colaborativa fue lo que nos permitió participar como socios de WikiLeaks en el proceso periodístico de los *GI Files*, con un medio regional, y a la vez, integrar este proceso participativo en nuestra investigación científica.

Hemos visto hasta aquí cómo el modelo de WikiLeaks ha evolucionado de las publicaciones en su sitio web de documentos en bruto que buscan eco mediático a un modelo periodístico tradicional que aplica previamente la selección, edición, contextualización y jerarquización de la información, en colaboración con organizaciones de noticias (Jones y Brown, 2011: 145), pero también con periodistas independientes, científicos y activistas que diversifican y amplifican la red de colaboradores de WikiLeaks.

[159] The Yes Men es un dúo de activistas formado por Andy Bichlbaum y Mike Bonanno que practica lo que llaman "corrección de identidad": desenmascarar a corporaciones multinacionales y a todo el entramado de intereses políticos y económicos tendentes a su protección, en perjuicio de los ciudadanos de todo el planeta. En: http://es.wikipedia.org/wiki/The_Yes_Men (último acceso: 21 de enero de 2013).

IV.5.4. Un modelo que se viraliza

Julian Assange y WikiLeaks, como sucede con los auténticos hackers, también son condenados en el discurso propagado desde las estructuras de poder tradicionales que penaliza y criminaliza a los hackers —la autoridad siempre se afana en sancionar a los librepensadores y disidentes (Goldstein, 2009: 550)—, y que anula la idea original de que son "héroes de la revolución informática" (Levy, 1984) con una ética y unos valores vinculados a la verdad, la libertad, la transparencia, el libre flujo de información y el acceso libre y universal al conocimiento. Pese a esto, el modelo WikiLeaks, adscrito a la ética hacker e inspirado en el modelo colaborativo de la economía moral de la información de los *wikis* —esto es, "un sentimiento de obligaciones mutuas y expectativas compartidas sobre lo que constituye una buena ciudadania en una comunidad de conocimientos" (Jenkins, 2008: 253)—, se ha viralizado y ha sido copiado por otros hackers, por medios de información y nuevas iniciativas ciudadanas en Internet. Aquí describimos sucintamente algunas de las primeras iniciativas que se pusieron en marcha siguiendo la estela de WikiLeaks, a finales de 2010 y durante el año 2011[160].

Una parte de Anonymous, unida en el grupo hacktivista People's Liberation Front, lanzó dos sitios web al estilo WikiLeaks para recibir filtraciones de hackers y de confidentes que quieran publicar informaciones sensibles: LocalLeaks.tk, que se centra en información de ámbito local, y HackerLeaks.tk, enfocada a todo el colectivo hacker que quiera publicar sus acciones. Localeaks.com es otro sitio de filtraciones, desarrollado a partir de un proyecto de investigación de la CUNY Graduate School's Entrepreneurial Journalism y dirigido a periódicos de pequeñas ciudades de Estados Unidos. BalkanLeaks.eu, IndoLeaks.org y BrusselsLeaks.com son otros de los numerosos clones locales y regionales de WikiLeaks que fueron apareciendo en todo el mundo. En España encontramos ejemplos como KanariLeaks.org, organización independiente sin ánimo de lucro que nació para llevar a cabo en una región concreta, las Islas Canarias, la tarea que WikiLeaks realiza en todo el mundo, y MiniLeaks.com,

[160] La mayoría de estos proyectos fueron finalmente desactivados. Sin embargo, consideramos que fueron de gran valor para expandir un nuevo modelo de periodismo de investigación basado en las comunicaciones seguras, la privacidad y la colaboración en red. Por eso, es importante su mención en esta tesis. Sitios de filtraciones actualmente activos, como Filtrala.org, que forma parte de la red internacional de la Associated Whistleblowing Press —organización no gubernamental sin ánimo de lucro, con sede en Bélgica, que se dedica a combatir la corrupción y violaciones de derechos humanos mediante el periodismo de investigación y herramientas para la transparencia—, deben su existencia a WikiLeaks, pero son fruto también de experiencias previas como las que describimos aquí.

un sitio que busca "promover la transparencia y honestidad en la sociedad a través de la publicación de documentación relevante", según explican en su página web.

El modelo WikiLeaks también ha causado gran fascinación en el sector de las empresas informativas. Algunos medios han intentado imitar este modelo, con más o menos suerte, pero sin alcanzar el estatus logrado por WikiLeaks: SafeHouse, de *The Wall Street Journal*; el servicio Transparency Unit, de Al Jazeera, y el sitio web FolhaLeaks, del diario *Folha de Sao Paulo*, son buenos ejemplos de esta tendencia a la que también se quiso sumar *The New York Times*, que anunció a principios de 2011 que estaba considerando la posibilidad de crear en un sitio web un "EZ Pass lane for leakers", es decir, una suerte de carril virtual especial para confidentes[161]. Pero a diferencia de estos medios, como bien explica Peter Scheer, director ejecutivo de la First Amendment Coalition[162], "Wikileaks es un hábil punto de venta de información que es a la vez apátrida y virtual", características que, "desafortunadamente para los medios de comunicación dominantes", dan a WikiLeaks "una ventaja permanente en la protección de documentos y fuentes confidenciales" (Scheer, 2011)[163]. Los denunciantes sólo están dispuestos a ofrecer información si su anonimato puede ser garantizado y protegido por leyes y por protocolos humanos y tecnológicos diseñados para tal fin. De su protección depende, en buena medida, la prevención y denuncia de fraudes y corrupción, la protección del medio ambiente, el reporte de crímenes y, en general, asegurar que la sociedad funcione bajo un marco jurídico y moral (Bell, 2011). Es en esa tarea en la que se centra WikiLeaks.

En el proceso de viralización del modelo WikiLeaks también han jugado un papel clave cientos de sitios web que le han prestado apoyo en todo el mundo creando espejos de la página de WikiLeaks, con el fin de contrarrestar los ataques informáticos a esta organización y garantizar, así, el acceso a los contenidos de WikiLeaks. El 15 de diciembre de 2010, en pleno apogeo del fenómeno WikiLeaks tras la publicación del *Cablegate*, el *site* de Information Clearing House había listado 2.194 sitios web espejos de WikiLeaks (véase Anexo I)

---

161 Véase: 'The Times Plans an EZ Pass Lane for Leakers', en http://www.forbes.com/sites/danbigman/2011/01/25/will-the-times-ez-pass-lane-for-leakers-flood-the-world-with-secrets/#691f842d468c (última consulta: 12 de enero de 2012).

162 First Amendment Coalition es una organización sin ánimo de lucro y de interés público en Estados Unidos, dedicada a la protección de la libertad de expresión, al impulso del gobierno abierto y responsable, y al fomento de la participación directa de los ciudadanos en los asuntos públicos.

163 Traducción propia.

Ilustración 25: Mapa 3D de Google Earth que muestra dónde se sitúan los espejos de WikiLeaks repartidos por todo el mundo y en España

Fuente: Laurence Muller, desarrollador de la Universidad de Harvard, en *Visualizing WikiLeaks Mirrors*: http://www.multigesture.net/2010/12/09/visualizing-wikileaks-mirrors/#demo (último acceso: 12 de enero de 2012).

IV.6. EL *STORYTELLING*

IV.6.1. Introducción

Desde que llegó a los grandes titulares de los medios de comunicación de masas y se viralizó en las redes sociales en línea, la historia de WikiLeaks y de su fundador, Julian Assange, se ha difundido en formas narrativas múltiples y cambiantes, moldeadas por las estructuras que articulan los grandes relatos ideológicos y por los críticos del sistema que ofrecen contranarrativas alternativas al discurso dominante (Uricchio, 2014: 2568).

Parecen varios los factores que contribuyen a la variedad e intensidad narrativa sobre el fenómeno WikiLeaks, principalmente: la liberación continua y sistemática de información filtrada, garantizando que la historia se mantenga en las portadas de los medios de comunicación y se desencandenen distintas series de respuestas partidistas; los muy diferentes significados e implicaciones de las filtraciones en diversos escenarios nacionales, lo que permite alimentar debates políticos locales, y una heterogénea gama de historias generadas en toda la prensa, también en la sensacionalista, desde informaciones sobre los documentos filtrados, hasta especulaciones sobre el comportamiento y la vida de Julian Assange (2014: 2568).

Precisamente, las narrativas sobre Assange han excitado si cabe aún más el maniqueísmo que domina, en general, el discurso político y, en particular, las interpretaciones del *hacking*, condenado al binarismo axiológico, a la simple dualidad maniquea del bien y del mal.

IV.6.2. Héroe *vs* Villano

La historia de Assange y de WikiLeaks es el resultado de una sucesión de narraciones diferentes, de una inmensa acumulación de historias propia de la vida de las sociedades neoliberales (Salmon, 2011). Uricchio considera que "en el caso de WikiLeaks es más correcto hablar de una red de relatos a veces en conflicto, con varias partes intentando dar forma y controlar la narrativa dominante" mediante el desarrollo de "un drama serializado" (Uricchio, 2014: 2567). Fabricar esta historia dramática se ha convertido en el gran reto de los *storytellers* políticos y mediáticos, expertos en desviar la atención de la opinión pública de un tema embarazoso.

> Si los gobiernos y las empresas afrontan revelaciones cada vez más embarazosas que no podrán contener, tendrán que reforzar también sus operaciones de *spin*. Dado que el impacto máximo de las revelaciones de WikiLeaks dependen a menudo de su interacción con los medios de comunicación tradicionales, en el mundo WikiLeaks el reinado de los *spin doctors* capaces de cambiar la agenda pública del día y generar distracciones puede ser más central que nunca para los gobiernos y las operaciones corporativas (Hood, 2011: 638)

Pero en su fabricación de la historia se han topado con nuevos *storytellers* que, de forma colaborativa, en red y en distintos soportes y medios, crean un relato distinto, antagónico al de los *storytellers* de la política oficial y de los medios tradicionales. A diferencia de lo que sucedió en las décadas de 1980 y 1990, ahora la versión oficial sobre el hacker villano se enfrenta a la del héroe en el mismo espacio —el ciberespacio— y en aparente igualdad de condiciones, al menos tecnológicas, decisivas en la disputa dialéctica. La contienda es narrativa y se extiende por los viejos y nuevos medios de comunicación, donde se desarrolla la gran batalla: la del mensaje; un mensaje que es, en ambos casos, político. La batalla adquiere nuevas formas de creación y difusión en el ciberespacio ubicuo y multicrónico, donde el potencial de viralización, casi hasta el infinito, amplifica el mensaje y alarga su impacto.

> Hoy en día el poder de internet multiplica la capacidad de expansión del relato porque aumenta la capacidad de los narradores, de las voces. Las posibilidades virales de la cultura digital pueden amplificar el mensaje implícito en el relato político, dada su capacidad de propagación, multiplicación y transmisión (Gutiérrez Rubí, 2011: 20).

Cada extremo narrativo proyecta en Julian Assange "superpedores de bonda o maldad" (Leigh y Harding, 2011: 21). Los periodistas de *The Guardian* que colaboraron directamente con él profundizan:

> La prensa y la opinión pública se dividieron entre aquellos que veían a Assange como una nueva especie de ciberMesías y los que lo consideraban como el villano de las películas de James Bond. Cada uno de estos extremos proyectaban en él superpoderes de bondad o maldad. El guión quedó todavía más confuso en diciembre [de 2010], cuando, como parte de las condiciones de su libertad bajo fianza, Asssange tuvo que trasladarse a vivir temporalmente a Ellingham Hall, una residencia georgiana situada en una amplia finca de la campiña de Suffolk. Era como si el autor de *Downton Abbey*[164], Julian Fellowes, hubiera adaptado un guión de Stieg Larsson (Leigh y Harding, 2011: 21)

164 Downton Abbey es una exitosa serie dramática de la televisión británica escrita por el guionista Julian Fellowes.

En medio de esta contienda, Assange —el protagonista bicéfalo, el héroe y villano— se posiciona como el gran estratega, como el supremo *storyteller* cuyo interés por mantener permanentemente la tensión narrativa sobre el fenómeno WikiLeaks le ha llevado a marcar los ritmos, a serializar el drama y a administrar los elementos de esta *wikistory* sobre el hombre que filtró el mundo y sobre su organización transnacional. Assange es el gran narrador omnisciente, omnipresente y omnipotente. "La relevancia de Julian Assange y su vida, marcada por su transformación en deidad o demonio, según las opiniones y los países, le ha permitido formatear su paisaje" (Plaza, 2011: 51). Assange sería otro nuevo "príncipe Sherezade, narrador de sí mismo. […] capaz de darse un aura novelesca, de mutar para convertirse en un sujeto intenso que adopta conductas memorables, dignas de ser contadas" (Salmon, 2011: 68).

El gran acierto estratégico de Julian Assange ha sido identificar WikiLeaks con su persona:

> Wikileaks es rentable en la medida en que Julian Assange queda asociado a ella, y su fundador ha pasado de anónimo y raro a mina de oro para la industria del ocio. Su historia vende; las historias que filtra, también, aunque da la impresión de que menos (Plaza, 2011: 52).

Assange se ha encargado de rodear su pasado de un halo de misterio. Una estrategia que anima a fantasear y a ingeniar parte de su vida, a especular sobre su personalidad, y, por tanto, a mitificar su figura a través de relatos que mezclan ficción y realidad, verdades y mentiras, asertos e inciertos, hechos y rumores, creencias y dudas, fe y razón. La historia de Julian Assange invita a la literatura (Plaza, 2011: 22).

El profesor Robert Manne hace hincapié en un detalle esencial en la narración de la vida de Julian Assange:

> Periodistas experimentados como David Leigh, del *Guardian*, o John F. Burns, del *New York Times*, en general aceptan como verdaderas muchas de las historias que Assange cuenta acerca de sí mismo. Ellos no entienden que, como muchos escritores, ha convertido su vida en una fábula (Manne, 2011).

Historias que Assange decidió empezar a contar junto con la periodista Suelette Dreyfus, con quien publicó *Underground*, obra fetiche del mundo hacker. Era 1997 y Assange ya sabía cuál debía ser su destino: convertirse en héroe mitológico. Comenzaban las escrituras sobre este *profeta* de la libertad en la era de la sociedad red;

un *storyteller* que en el prólogo de *Underground* introdujo el siguiente aforismo de Oscar Wilde, que le ha acompañado hasta ahora: "El hombre es menos uno mismo cuando habla en primera persona. Dale una máscara y te dirá la verdad" (Wilde es uno de los personajes históricos más recurridos en la historia de Assange).

El relato sobre Julian Assange y WikiLeaks es construido en múltiples medios por múltiples narradores: el autodiegético (Julian Assange), el homodiegético (los socios y ex socios de WikiLeaks, los periodistas que colaboraron con la organización y los allegados de Assange) y el heterodiegético (analistas, periodistas, políticos, escritores, cineastas y fans y detractores que han construido sus relatos sobre el fundador de WikiLeaks). En esta línea, Mónica Plaza señala:

> Estando vivo y siendo capaz de alterar a golpe de teclado su presente y su destino, nada impide que el fundador de WikiLeaks pueda cambiar cuando lo desee su pasado. Así, hablar de él es remitirse a otros autores, a declaraciones de aquí y de allá que hicieron en su momento vecinos, amigos o familiares, a una sucesión de reseñas que, combinadas, ofrecen la panorámica de Julian Assange (Plaza, 2011: 22).

En la construcción de esta historia policonstruida han jugado también un papel determinante la estética a la que ha recurrido Assange y sus puestas en escena.

> Con su tez fantasmal, su lacio pelo blanco (cuando no está teñido o cortado para ocultar su identidad) y su monocorde sonsonete grave, Assange no sólo se comporta como un personaje surgido a la vida de un guión de ciencia ficción, sino que incluso se ve y suena como un personaje de ciencia ficción (Hosenball, 2010)[165].

Assange ha llevado una vida digna de un *best-seller* de espías: ha vivido casi en la clandestinidad, saltando de país a país, alojándose en casas de amigos y partidarios, negándose a decir de dónde viene y adónde irá, cambiando a menudo sus números de teléfono, que sólo da a unos pocos, o usando sistemas de encriptación en sus comunicaciones. "Nunca se sabe dónde está, dónde dormirá esta noche, o en qué anda. Su vida nada en los secretos. Se mueve rápido y procura no dejar rastro" (Elola, 2010). Alto, delgado, albino, sofisticado cuando la ocasión lo requiere, a veces con una leve sonrisa pícara que raya la ironía y aspecto de nuevo dandi posmoderno en sus comparecencias públicas, Julian Assange pesa cada palabra con una voz cavernosa, pausada y monocorde, a veces difícilmente audible, y se muestra casi siempre

[165] Traducción propia.

imperturbable en sus apariciones públicas. Lidera la franquicia de la democracia y de la libertad de expresión y de información en el ciberespacio: WikiLeaks.

Como ya hemos dicho, la suya es una *wikistory* con dos grandes argumentos: el del villano que pone en peligro la seguridad de los Estado-nación y de ciudadanos, y el del héroe que lucha por la democracia, la libertad de expresión y la transparencia informativa. Adaptando el esquema propuesto por el consultor de comunicación Antonio Núñez (2007) sobre la técnica del *storytelling*, a la vez inspirado en las propuestas sobre la estructura del cuento de Vladimir Propp, así es como vemos que se construyen estos dos grandes relatos:

Cuadro 9: *Storytelling* aplicado a Julian Assange.

	Agravio	Héroe	Villano	Objeto mágico	Aprendizaje	Duelo final	Sancion social
storytelling 1	Control y manipulacion de la información	Julian Assange	Estado-nación	Tecnología punta de codificación	Filtraciones	Libertad de expresión y transparencia informativa	Assange es declarado héroe
storytelling 2	Abusos sexuales Poner en riesgo la seguridad del Estado-Nación	Estado-nación	Julian Assange	Orden de detención y de extradición	Acoso político, judicial y económico	Detención de Assange y paralización de Wikileaks	Assange es declarado villano

Fuente: elaboración propia.

En el *storytelling* del Assange villano participan sus detractores y acusadores, entre los que encontramos a los tres poderes tradicionales (ejecutivo, legislativo y judicial), al cuarto poder que representan los medios de comunicación dominantes (algunos de ellos, exaliados de WikiLeaks) y a excolaboradores directos de Assange. Le tachan de delincuente informático, espía, ciberterrorista, anarquista, ladrón, prófugo de la justicia, sucio y egocentrista. Acusaciones que calan muy bien en la opinión pública, porque "la gente quiere villanos claramente definidos y soluciones excesivamente simplistas y satisfactorias" (2009: 258). El nuevo villano es el enemigo público número uno de los Estados-nación, buscado por la Interpol:

> Interpol ha emitido una «circular roja» para su arresto en nombre de las autoridades suecas, con el objeto de interrogarle en relación a «varios abusos sexuales» —Gadafi, acusado de crímenes de guerra, sólo mereció una «circular naranja»— y el gobierno estadounidense le ha marcado como «terrorista tecnológico». (Hastings, 2012: 48).

Ilustración 26: Orden de detención de Assange emitida por Interpol.

Fuente: página web de Interpol http://www.interpol.int/.

Para el fundador de WikiLeaks, su caso fue diseñado por los ingenieros del *storytelling* político: "Están intentando crear un caso de espionaje contra mí y otros miembros de la organización, y contra gente que ha tenido relación con nosotros en Estados Unidos", denunció en una entrevista concedida a Joseba Elola para el *El País*, publicada el 24 de octubre de 2010.

Periódicos como *El País* y *The Guardian* aplicaron el modelo del *transmedia storytelling* para contar la historia del *Cablegate* a través de múltiples plataformas, diferentes formatos de contenidos y participación activa del público en la elaboración de entrevistas y recomendación de pasajes de la narración (Dias Souza, 2011). Pero han sido principalmente las autoridades políticas y militares estadounidenses las que han entremezclado en el debate argumentos que apelan a la razón y a las emociones y sentimientos patrióticos de los ciudadanos (Leigh y Harding, 2011).

Como consecuencia directa de las publicaciones de WikiLeaks, el Gobierno de Estados Unidos inició una investigación criminal multiagencia sobre Julian Assange, el personal de WikiLeaks, sus partidarios y colaboradores (Assange *et al.*, 2012: 13-14).

WikiLeaks había logrado humillar, o al menos ruborizar, a la mayor superpotencia del mundo, Estados Unidos, con las filtraciones de documentos de las guerras de Irak y Afganistán, y de los cables diplomáticos entre sus embajadas y el Pentágono. El jefe de la Comisión de Seguridad Nacional del Senado de Estados Unidos, el demócrata Joe Lieberman, declaró que WikiLeaks estaba poniendo en peligro la vida y la libertad de innumerables estadounidenses y no estadounidenses por todo el mundo:

> Se trata de una acción escandalosa, temeraria, y despreciable que socavará la capacidad de nuestro Gobierno y de nuestros socios para proteger a nuestra gente y para trabajar juntos para defender nuestros intereses vitales. Que no haya dudas: los responsables van a tener sangre en sus manos (Lieberman, en Condon, 2010).

Mike Mullen, jefe del Estado Mayor Conjunto de Estados Unidos, sugirió anteriormente que WikiLeaks "podría tener ya en sus manos la sangre de algún joven soldado o la de una familia afgana" (Leigh, 2010). El presidente del Comité de Seguridad Nacional de la Cámara de representantes estadounidense, el republicano Peter King, fue más allá, solicitando que WikiLeaks fuera considerada una organización terrorista y pidiendo al Fiscal General, Eric Holder, que pusiera a Assange bajo la Ley de Espionaje (Epstein, 2010). El vicepresidente Joe Biden llamó a Assange "terrorista de alta tecnología" (MacAskill, 2010). La polémica exgobernadora ultraderechista de Alaska y excandidata republicana a la vicepresidencia de Estados Unidos en 2008, Sarah Palin, pidió a través de su página en Facebook que la Administración Obama persiguiese a Assange "con la misma urgencia" con la que se se perseguía a los líderes del grupo terrorista Al Qaeda y de los talibanes (Palin, 2010). El profesor de la University of Calgary Thomas Eugene Flanagan, que había sido asesor del primer ministro de Canadá Stephen Harper, sugirió en una entrevista en CBC News Network que Assange debía ser asesinado, declaraciones de las que luego se arrepintió, aunque que debía ser detenido (CBC News, 2010). El precandidato presidencial republicano estadounidense Mike Huckabee también pidió su ejecución (Siddique y Weaver, 2010).

A la vez, Visa, Mastercard y PayPal cortaron relaciones con WikiLeaks por la presión política. Y Amazon eliminó a WikiLeaks de sus servidores después de una llamada telefónica del senador Lieberman. Al respecto, Assange explica:

> En un acto de censura a una agencia periodística sin precedentes, el Gobierno de Estados Unidos presionó a los servidores de Internet para que dejaran de dar servicio a Wikileaks.org. El 1 de diciembre de 2010, Amazon eliminó a WikiLeaks de sus

> servidores de almacenamiento y el 2 de diciembre, el servidor DNS (sistema de nombres de dominio) asignado al dominio de Wikileaks.org fue atacado. WikiLeaks se mantuvo en la red durante este periodo gracias a la creación masiva de *espejos*, por medio de los cuales miles de seguidores de WikiLeaks copiaban el sitio web y alojaban su propia versión distribuyendo las direcciones IP a través de las redes sociales (Assange *et al.*, 2012: 15).

Los niveles de paranoia política se dispararon tras las filtraciones de cables diplomáticos de Estados Unidos:

> En diciembre de 2012, a raíz de las filtraciones del caso *Cablegate*, varios políticos plantearon enérgicamente el asesinato extrajudicial de Julian Assange, llegando a proponer la utilización de aviones no tripulados. Senadores norteamericanos calificaron a WikiLeaks de «organización terrorista», tildando a Assange de «terrorista tecnológico» y «combatiente enemigo» involucrado en la «ciberguerra» (Assange et al., 2012: 14).

El Gobierno estadounidense abrió cinco frentes: uno, contra WikiLeaks y Julian Assange; otro contra toda cualquier persona física o jurídica que prestase cualquier tipo de soporte a WikiLeaks; también contra los medios y periodistas que ejerciesen de altavoces de las denuncias de WikiLeaks, y por último, contra cualquier individuo que tuviese intención de usar el material filtrado; es decir, los cinco sujetos de derecho que Braman (2014) identifica en las complejas cuestiones legales que plantea este caso. Especialmente controvertidas fueron las actuaciones contra periodistas y medios de información, como recuerda Assange:

> Las audiencias del Comité del Congreso vienen escuchando […] la propuesta por parte de algunos miembros del Congreso de Estados Unidos de que la Ley de Espionaje se utilice como herramienta para procesar a periodistas que «deliberadamente publiquen información confidencial», sugiriendo que el enfoque se institucionalice en el sistema de justicia estadounidense (Assange *et al.*, 2012: 13).

En concreto, varios miembros del Subcomité de Crimen, Terrorismo y Seguridad Nacional, del Comité Judicial del Congreso de Estados Unidos, propusieron actuar contra los periodistas que estaban publicando información basada en las filtraciones de documentos secretos, para que revelasen sus fuentes (Miller, 2012).

Los controles se extendieron a empleados federales y al ámbito académico:

> […] la Administración Obama ordenó a los empleados federales que mantuvieran como «clasificado» el material filtrado por WikiLeaks, pese a que esta información estaba siendo publicada por algunas de las agencias de noticias más

> importantes del mundo, incluidos los diarios *The New York Times* y *The Guardian*. Los empleados recibieron la consigna de que el acceso al material, ya fuera a través de Wikileaks.org o de *The New York Times*, se consideraría violación de la seguridad. Tanto las agencias gubernamentales como la Biblioteca del Congreso, el Departamento de Comercio y el Ejército de Estados Unidos bloquearon el acceso al material de WikiLeaks a través de sus respectivas redes. La prohibición no se limitaba únicamente al sector público. Los empleados del Gobierno de Estados Unidos advirtieron a las instituciones académicas de que los estudiantes que quisieran hacer carrera en el sector público debían evitar todo contacto con las informaciones reveladas por WikiLeaks en sus investigaciones y en su actividad *online* (Assange *et al.*, 2012: 15).

Al mismo tiempo, se emprendió una campaña de acoso contra aquellos individuos destacados en el entorno de WikiLeaks. Al igual que sucedió en la segunda mitad de la década de 1980 y durante los años noventa contra numerosos hackers, los resortes de la seguridad nacional se accionaron contra cualquier hacktivista vinculado directa o indirectamente a WikiLeaks. Veamos algunos ejemplos destacados.

Para el 17 de julio de 2012 estaba programada una charla de Julian Assange en la tradicional conferencia Hackers on Planet Earth (HOPE) que organiza cada año en Nueva York la revista *2600*. Assange tuvo que cancelar su intervención y Jacob Appelbaum participó en su lugar como portavoz de WikiLeaks. A partir de entonces se activó toda una campaña de acoso y derribo contra Appelbaum y las personas de su entorno.

> Desde entonces, Appelbaum es objeto de frecuentes detenciones e investigaciones, denegándosele cualquier tipo de asistencia jurídica y siendo sometido a interrogatorios en la aduana cada vez que entra y sale de Estados Unidos. Su equipo ha sido confiscado y sus derechos, violados en repetidas ocasiones bajo la amenaza de acciones similares futuras. En esta persecución han participado docenas de agencias gubernamentales, desde el Departamento de Seguridad Interna, Inmigración y Aduanas, hasta el Ejército estadounidense. Las detenciones han incluido además la prohibición de acceder al cuarto de baño como método de presión. Appelbaum no ha sido nunca acusado formalmente ni ha recibido explicación alguna por parte del Gobierno sobre las razones del acoso que viene padeciendo (Assange *et al*., 2012: 17).

¿Por qué tanto interés en este hacktivista? ¿Qué relevancia tiene para las autoridades? Appelbaum es un periodista independiente, miembro del grupo hacktivista Cult of the Dead Cow desde el año 2008, fundador del *hackerspace* Noisebridge en San Francisco, colaborador del Chaos Cumputer Club alemán y desarrollador informático. Es, además, uno de los principales defensores e investigadores del Proyecto Tor, el sistema de anonimato virtual creado para que cualquier usuario pueda evitar la

vigilancia y sortear la censura en Internet usando una red de comunicaciones encriptadas. También ha destacado en su ayuda a activistas medioambientales y de los derechos humanos. Appelbaum ha publicado numerosos e innovadores estudios sobre seguridad, privacidad y anonimato en la Red. Está, además, convencido de que todos, sin excepción, tenemos derecho a acceder a la información y a expresarnos libremente, sin ningún tipo de restricción. Appelbaum colaboró también intensamente en la publicación de documentos secretos revelados por Edward Snowden en junio de 2013.

> En el año 2010, cuando a Julian Assange se le prohibió dar una charla en Nueva York, Jacob la impartió en su lugar. Desde entonces él, sus amigos y su familia han sido sistemáticamente acosados por el Gobierno de los Estados Unidos: interrogados en aeropuertos, sometidos a agresivos cacheos y amenazas ilegales de prisión inminente por parte de agentes de la ley, su equipo ha sido confiscado y sus servicios en la Red han sido objeto de numerosas citaciones secretas. A Jacob no le amedrentan estas medidas y prosigue con sus múltiples batallas legales; erigido en ferviente defensor de la libertad de expresión, es una de las voces más elocuentes de WikiLeaks (Assange *et al.*, 2012: 8).

Otra víctima de la persecución de las autoridades a personas influyentes del entorno de Assange ha sido Jérémie Zimmermann.

> A mediados de junio del año 2011, cuando se disponía a embarcar en un avión en el aeropuerto Dulles de Washington, Jérémie Zimmermann fue abordado por dos hombres que se identificaron como agentes del FBI. Estos agentes le hicieron preguntas sobre WikiLeaks y le amenazaron con detenerlo y encarcelarlo (Assange *et al.*, 2012: 17).

Zimmerman es el cofundador y portavoz del grupo La Quadrature du Net, una de las organizaciones europeas más importantes en el ejercicio de la defensa del derecho al anonimato en la Red y en el trabajo para concienciar a la población sobre la existencia de ataques normativos a las libertades en el ciberespacio. Zimmerman trabaja para construir herramientas que permitan la participación de los individuos en el debate público e intentar así producir cambios en el sistema. Está tremendamente implicado en las guerras de derechos de autor, en el debate sobre la neutralidad de la Red y en otras cuestiones legales cruciales para el futuro de una Internet libre. Su grupo La Quadrature du Net lideró una campaña pública de rechazo en el Parlamento Europeo al Acuerdo Comercial de la Lucha contra la Falsificación (Anti-Counterfeiting Trade Agreement, conocido como ACTA), aunque finalmente fue firmado por la Unión Europea en 2012 para garantizar la protección de los derechos de propiedad intelectual. Poco después de

participar en el debate que sentó las bases del libro *Cypherpunks* (2012) —junto con Assaange, Appelbaum y Müller-Maguhn— Zimmerman fue abordado por dos agentes del FBI cuando abandonaba Estados Unidos e interrogado acerca de WikiLeaks.

> Appelbaum y Zimmermann se encuentran en la lista de amigos, seguidores o presuntos colaboradores de Julian Assange que han sido objeto del acoso y vigilancia por parte de agencias gubernamentales estadounidenses, una lista que incluye a abogados y periodistas que se limitan a hacer su trabajo (Assange *et al*., 2012: 17).

La campaña contra WikiLeaks se extendió incluso a las redes sociales. El 14 de diciembre de 2010, Twitter recibió una citación administrativa del Departamento de Justicia de Estados Unidos en la que se instaba a los responsables de esta plataforma a suministrar información relacionada con la investigación abierta sobre WikiLeaks, en concreto, de las cuentas en esta red social de Julian Assange y de varios de sus colaboradores. La citación se presentó al amparo de la Stored Communications Act, por la que el Gobierno de Estados Unidos se declara competente para exigir la revelación de comunicaciones electrónicas privadas sin necesidad de que un juez dicte una orden de registro, sentando así las bases legales para sortear las protecciones conferidas por la Cuarta Enmienda frente al registro e incautación arbitrarios. La citación requería nombres de usuario, correos electrónicos, direcciones IP, números de teléfono, cuentas bancarias y números de tarjetas asociados con cuentas y personas presuntamente relacionadas con WikiLeaks, incluidos Jacob Appelbaum, la parlamentaria islandesa Birgitta Jónsdóttir, el empresario holandés y pionero de Internet Rop Gonggrijp, además de los propios datos de WikiLeaks y Assange y del soldado Manning. Según los términos de la citación, Twitter no podía bajo ningún concepto comunicar su existencia a los interesados.

Twitter recurrió con éxito esta prohibición y consiguió que se le reconociera el derecho de informar a estas personas de la confiscación de sus archivos. Se lo notificó el 5 de enero de 2011. El 26 de enero, Appelbaum, Jónsdóttir y Gonggrijp, representados por la firma Kecker & Van Nest, la American Civil Liberties Union y la Electronic Frontier Foundation, convocaron a sus respectivos abogados para interponer un recurso de nulidad contra dicha orden. Además, el abogado de Appelbaum presentó un nuevo recurso en el que solicitaba la desclasificación de los expedientes judiciales que revelaban los intentos gubernamentales de recabar información privada de Twitter y de

otras compañías que podían haber sido objeto de estas mismas presiones por parte del Gobierno estadounidense sin orden judicial. Ambos recursos fueron desestimados el 11 de marzo de 2011 por la jueza del tribunal de Alexandria (Virginia) Theresa Carroll Buchanan (Alandete, 2011). Los demandantes apelaron esta resolución.

El 10 de octubre de 2011, el diario *The Wall Street Journal* reveló que Google y el servidor californiano Sonic.net habían recibido una citación similar del Gobierno de Estados Unidos solicitando información de las cuentas de correo electrónico de Appelbaum, en concreto, las direcciones de las cuentas de correo con las que había contactado en los dos últimos años. Sonic.net recurrió la orden ante un tribunal y perdió. Las dos compañías obtuvieron permiso para comunicar a Appelbaum que habían sido obligadas a remitir información sobre su correo electrónico (Angwin, 2011).

El 10 de noviembre de 2011, el juez de distrito Liam O'Grady se pronunció en contra de Appelbaum, Jónsdóttir y Gonggrijp al dictaminar que Twitter debía suministrar la información de sus cuentas al Departamento de Justicia (Assange *et al*., 2012: 18-19, 54; Sengupta, 2010).

Assange, Zimmermann, Appelbaum, Manning, Snowden. Al igual que los hackers de finales del siglo XX, los hacktivistas de hoy y sus colaboradores son perseguidos y acosados por la autoridad, aunque con repercusiones aún más graves y globales. Este despliegue de una retórica agresiva, incluso violenta, articulada por el poder político de Estados Unidos, y la ejecución de acciones represivas y de censura contra los nuevos disidentes, han sido interpretados por las corrientes periodística y académica más críticas como una profunda demostración del autoritarismo del Estado y de su capacidad sancionadora (Springer *et al.*, 2012), y como un ataque directo a la libertad de prensa y de expresión.

Las manifestaciones a favor de la censura y del control de la prensa no se han disimulado. Así, por ejemplo, el senador utraconservador por Carolina del Sur Trey Gowdy defiendió, a raíz del caso WikiLeaks, que no existe ninguna ley federal que sirva de escudo para proteger a los periodistas y que los derechos de la Primera Enmienda no son absolutos. El senador llegó a decir: "La idea de que la Primera Enmienda no tiene limitaciones es un disparate, legalmente y de cualquier otra manera" (Miller, 2012). Por su parte, el fiscal Kenneth L. Wainstein, posicionado a favor de la reforma de la Ley de Espionaje, "argumentó que la función que cumplen los periodistas será «menos

enérgica» si tienen que enfrentarse a mayores posibilidades de ser citados judicialmente" (Miller, 2012).

El último pilar de la estrategia de acoso y derribo de la Administración Obama fue la asfixia económica de WikiLeaks, estrangulando todas las vías de financiación de WikiLeaks. Tradicionalmente, el poder político, pero también el corporativo, han intentado controlar o acallar las voces de los medios críticos, bien mediante la concesión de ayudas económicas en forma de subvención, publicidad, patrocinio, financiación, etc., para comprar voluntades, o bien mediante la estrangulación de su economía con leyes *ad hoc*, confiscaciones, cierres judiciales, retirada de ayudas y de inversiones, presiones al mercado, etc. Pero WikiLeaks se muestra como un caso singular, ya que se trata del primer gran bloqueo económico *ciberespacial* por motivos políticos. Un bloqueo en el que están implicadas empresas del capitalismo financiero y del capitalismo tecnológico.

> WikiLeaks se financia a través de donaciones. En diciembre de 2010, instituciones bancarias y financieras, incluidas VISA, MasterCard, Paypal y el Bank of America, cedieron a las presiones oficiosas de Estados Unidos y empezaron a denegar servicios financieros a WikiLeaks. Bloquearon las transferencias bancarias y todas las donaciones efectuadas con las principales tarjetas de crédito. Dado que todas ellas son instituciones norteamericanas, su ubicuidad en el mundo financiero derivó en que a muchos donantes, tanto de Estados Unidos como del resto del mundo, se les denegó la opción de enviar dinero a WikiLeaks para financiar su actividad periodística. El bloqueo bancario, así se le conoce, se está llevando a cabo al margen de procedimiento judicial o administrativo alguno (2012: 16).

WikiLeaks, carente de ingresos y con costes que sufragar, tuvo que empezar a operar con fondos de reserva desde el inicio del bloqueo, en diciembre de 2010. Esta interrupción de los flujos de financiación de WikiLeaks ha sido explicada como un método de censura y un ataque al libre mercado efectivo que reclaman los *cypherpunks*.

> El bloqueo bancario es una reafirmación del poder que controla las transacciones económicas entre terceros. Menoscaba sin cortapisas las libertades económicas de los individuos. Va incluso más allá: la amenaza existencial que supone para WikiLeaks representa una nueva y preocupante forma de censura económica global (Assange *et al:*, 2012: 16).

En definitiva, lo que se puso en marcha fue la vieja táctica de matar al mensajero (Elías, 2011). Para justificarlo, la estrategia ha sido desviar la atención del mensaje, focalizando el discurso político y mediático sobre la figura del fundador de

WikiLeaks, ahondando en su intrincada personalidad, en sus aventuras y desventuras, en sus obsesiones, en su ideología, etc. Assange fue fundido en múltiples personajes villanos, caracterizaciones que eclipsaron las filtraciones y reconceptualizaron la liberación de documentos secretos como actos irresponsables de un individuo retorcido con aspiraciones maliciosas (Uricchio, 2014: 2569). Discursos basados en cuestiones éticas y estéticas han pretendido desprestigiar y criminalizar a Assange y presentarlo ante la opinión pública mundial como un nómada desarraigado y marginal, con tintes megalómanos, capaz de dañar la dignidad y la integridad física de dos mujeres en presuntos casos de abusos y violación en Suecia, y de poner en peligro las vidas de personas en zonas de conflicto en todo el mundo y la seguridad de los Estados-nación. Se quita así el foco de atención del mensaje, de los datos y los hechos filtrados, y se pone el foco sobre el mensajero para asesinar su reputación y debilitar su fiabilidad.

> Los relatos escritos por los departamentos de Estado y de Defensa de Estados Unidos, y distribuidos a la prensa y los socios diplomáticos, fueron socavados por informes confidenciales que dieron pruebas de sus motivos y acciones reales.
>
> En segundo lugar, el Gobierno, dado que no puede impugnar la credibilidad de los documentos filtrados y es incapaz de impedir el potencial de distribución de Internet y el efecto resonador de la prensa internacional, se embarcó en una estrategia de personalización de WikiLeaks, equiparándola con Julian Assange, y luego mostrando que era Assange el narrador poco fiable (Uricchio, 2014: 2569).

Al mismo tiempo, Assange y sus partidarios presentan también al Gobierno de Estados Unidos y a sus aliados como narradores de nula confianza, con patrones de comportamiento engañosos como los que evidencian las filtraciones (Uricchio, 2014: 2570). Assange identifica al Estado-nación como el enemigo de las libertades del individuo. Para el fundador de WikiLeaks, "los Estados son sistemas a través de los cuales fluyen fuerzas coercitivas" (Assange et all. 2012: 2). Más claramente, expone:

> Facciones dentro de un Estado pueden competir por apoyos, lo que conduce al fenómeno de la democracia aparente, pero los fundamentos de los Estados son aplicar y evitar de modo sistemático la violencia. La propiedad de las tierras, los bienes, las rentas, los dividendos, los impuestos, las multas, la censura, los derechos de autor y las marcas registradas son impuestos por la amenaza de aplicar la violencia estatal. La mayor parte del tiempo no somos conscientes siquiera de lo cerca que estamos de la violencia, porque todos hacemos concesiones para evitarla (Assange *et al.*, 2012: 2-3).

Julian Assange considera que no hay otra forma posible de conocer realmente al enemigo que yendo a su encuentro para plantarle cara. Y es sólo la experiencia del

encuentro directo con el adversario lo que otorga potestad para guiar la resistencia. Así lo explicita el fundador de WikiLeaks:

> Si bien muchos escritores han considerado lo que significa Internet para la civilización mundial, están equivocados. Se equivocan porque no tienen el sentido de la perspectiva que aporta la experiencia directa. Se equivocan porque nunca han conocido al enemigo.
>
> Ninguna descripción del mundo sobrevive al primer contacto con el enemigo.
>
> Nosotros hemos conocido al enemigo.
>
> En los últimos seis años, WikiLeaks ha tenido conflictos con casi todos los Estados poderosos. Conocemos por dentro el nuevo estado de vigilancia porque hemos sondeado sus secretos. (Assange *et al.*, 2012: 1-2).

Para hacer frente a sus enemigos, WikiLeaks asume y practica la actitud combativa tradicional de los hacktivistas y también propia de los disidentes, con un léxico bélico que contribuye a dramatizar un conflicto en el que Julian e Assange justifica las acciones de de su organización de filtraciones como un ejercicio de la legítima defensa.

> Conocemos [el estado de vigilancia] desde la perspectiva del combatiente, porque hemos tenido que proteger de éste a nuestra gente, nuestras finanzas y nuestras. Lo conocemos desde una perspectiva global, porque tenemos personas, activos e información en casi todos los países. Lo conocemos desde la perspectiva del tiempo, porque hemos estado luchando contra este fenómeno desde hace años y lo hemos visto duplicarse y extenderse una y otra vez. Es un parásito invasivo que engorda a costa de las sociedades que entran en contacto con Internet. Se está extendiendo por el planeta, infectando a todos los Estados y pueblos a su paso (Axssange *et al.*, 2012: 2).

Para combatir al Estado-nación, los *cypherpunks* como Assange proponen el uso de la criptografía como el objeto mágico que resuelve el conflicto a favor de quien lo utiliza.

> La criptografía es el *súmmum* de las leyes de la la física, y no escucha ni las bravatas de los Estados ni las distopías de la vigilancia transnacional. No es obvio que el mundo tenga que funcionar de esta forma. Pero, de alguna manera, el universo sonríe a la encriptación. La criptografía es la última forma de acción directa no violenta […]. Una criptografía sólida puede resistir la aplicación de una violencia ilimitada. Ninguna fuerza coercitiva podrá nunca resolver un problema matemático (Assange et al., 2012: 5).

Esta afirmación es ratificada por Appelbaum, quien aboga por democratizar la criptografía como arma de defensa ciudadana:

> La fuerza de casi todas las autoridades modernas se deriva de la violencia y de la amenaza de violencia. Debemos asumir que con la criptografía ningún tipo de violencia resolverá nunca un problema matemático […] Sin embargo, esto es algo que no resulta en absoluto evidente para el común de los mortales y tenemos que hacérselo entender. Si todos pudiésemos resolver todos esos problemas matemáticos sería otra historia y, por supuesto, el gobierno también podría hacerlo (Assange *et al.*, 2012: 61).

Por lo tanto, la fuerza del nuevo mundo que se quiere construir reside en las matemáticas. Assange profundiza aún más en esta idea de la criptografía computacional como un instrumento matemático complejo de legítima defensa:

> El caso es que es parte de nuestra realidad, como lo es el hecho de que se pueden fabricar bombas atómicas, que podemos crear problemas matemáticos que ni siquiera las mayores potencias son capaces de descifrar. Creo que eso caló tremendamente en los libertarios californianos y otros grupos que creían en este tipo de idea de «democracia cargada y con el seguro puesto», porque aquí planteábamos hacerlo por la vía intelectual: la de un par de individuos con criptografía enfrentándose al poderío de la mayor potencia del mundo. Así que el universo tiene una propiedad que está del lado de la privacidad, porque existen algunos algoritmos criptográficos que ningún gobierno podrá romper jamás (Asange *et al.*, 2012: 61-62).

En el uso de la criptografía, en la revelación de secretos y en la defensa del libre flujo de información subyace una actitud antisistema que el propio Assange exhibe sin ambages:

> Nuestra tarea es asegurar la libre determinación donde podamos, contener la inminente distopía donde no podamos y, si todo falla, acelerar su autodestrucción (Assange *et al.*, 2012: 6).

Y en ese propósito, Assange no está solo.

IV.6.3. Un disidente con una legión de seguidores

Julian Assange se ha erigido en el adalid de la nueva disidencia hiperespacial, de los insurrectos involucrados en una batalla por el futuro de la humanidad en la que el individuo, finalmente, triunfaría. Assange se coloca así como un Winston Smith que, en esta ocasión sí, vencería en la próxima batalla al Gran Hermano. "Es David contra Goliat, es el hombre que lleva el mensaje de 1984 de Orwell a la era digital, es el héroe de una novela de Solzhenitsyn" (Lo Dico, 2011)[166].

[166] Traducción propia.

Assange simboliza y encarna la disidencia de una nueva generación transnacional de hacktivistas. El fundador de WikiLeaks ejemplifica la fuerza disruptiva del disidente y su emancipación subversiva. En los propios documentos internos de WikiLeaks, Assange alega que sus raíces están en comunidades disidentes (WikiLeaks Leak, 2007). Y la figura del disidente siempre ha generado una enorme fascinación en la cultura occidental. Tanta, que incluso hay un cierto encanto contraindicado en ser un (ciber)villano a ojos del Estado-nación (Goldstein, 2009: 260).

> Assange […] podría ser el nuevo Galileo del siglo XXI. No en el sentido intelectual —a pesar de que Assange estudió Física y Matemáticas como Galileo— sino en su confirmación como el disidente de la corriente dominante. Esa que cree que los estados deben y pueden ocultar información. Se arriesga a pena de muerte, simplemente, por publicar algo. Eso también le sucedió a Galileo (Elías, 2011).

Esto entronca con el argumento expuesto por el filósofo Slavoj Žižek en el encuentro que mantuvo con Julian Assange organizado por Democracy Now! en julio de 2011, en el que el filósofo esloveno concluyó que la fuerza disruptiva de Assange radica en su capacidad de alterar la subversión y llevar a la disidencia por nuevos caminos:

> No confundan a Julian y su banda […] con el heroísmo burgués de siempre; el de la lucha por el periodismo de investigación, el libre flujo de la información y todo eso. Lo que están haciendo es mucho más radical. Por eso ha generado tanto resentimiento: no sólo están violando las reglas y revelando secretos. La prensa burguesa, a la vieja usanza marxista, tiene sus propias maneras de ser transgresora. Su ideología no sólo controla lo que uno puede decir, sino también cómo uno puede violar aquello que tiene permitido decir. Usted [Julian Assange] no está violando las reglas, está cambiando las mismas reglas acerca de cómo tenemos permitido violar estas reglas. Esto es seguramente lo más importante que usted puede hacer (Democracy Now!, 2011).

Los ataques y críticas a WikiLeaks han tenido un efecto paradójico. En lugar de mitigar su impacto, han provocado masivas reacciones de apoyo a la organización y a su fundador en las calles de muchas ciudades y, sobre todo, en el ciberespacio.

A la par que las críticas, presiones, censura y acoso a WikiLeaks por parte del Gobierno de Estados Unidos han ido *in crescendo*, y sus presiones a los proveedores de servicios financieros y tecnológicos han ido surtiendo efecto para intentar paralizar a esta organización, también ha crecido el apoyo a WikiLeaks, con miles de internautas

en movimientos espontáneos como la campaña *Free WikiLeaks*[167], que se viralizó por todo el mundo y que recuerda a la campaña 'Free Kevin' que puso en marcha la revista *2600* a finales del siglo XX para la liberación del hacker Kevin Mitnick.

Además, el uso de software de fácil acceso y de protocolos de intercambio de archivos como BitTorrent, o los miles de *espejos* web creados, han evidenciado la imposibilidad de detener un fenómeno global como éste en la Red. "Cualquier esfuerzo por meter al genio en la botella es siempre inútil en la era de Internet", advierte el analista tecnológico Carmi Levy en declaraciones recogidas el 5 de diciembre de 2010 por *The Globe and Mail*, dos días antes de la detención de Julian Assange en Londres. Para Levy ya no tiene tanta trascendencia que WikiLeaks pueda ser bloqueado e inutilizado, porque "los datos ya están ahí fuera" (El Akkad, 2010) y han generado una reacción.

> El aluvión de reacciones contrarias a la detención del australiano llevó a que #wikileaks y #assange, entre otros *hashtags*, permanecieran en el *top* de los *trending topics* de Twitter durante varios días. WikiLeaks capitalizó la conversación en la plataforma de *microblogging* con el relato minuto a minuto de todos los acontecimientos relacionados con el arresto de Assange (Yuste, 2011).

Las campañas a favor de WikiLeaks y de Julian Assange emulan aquéllas que se pusieron en marcha en la década de 1990 a favor de hackers acosados y encarcelados. Por ejemplo: la campaña 'Free Kevin' que en 1998 auspició la revista *2600* para la liberación de Kevin Mitnick, con la que consiguió recaudar tres mil dólares para la defensa del hacker mediante la venta de miles de pegatinas y el lanzamiento del sitio www.kevinmitnick.com[168] (Goldstein, 2009: 566). Sin embargo, el desarrollo de la web social y la penetración de Internet en todo el planeta ha permitido a WikiLeaks un soporte sin precedentes en la historia. Nuevas voces se han ido sumando a las que ya habían manifestado su defensa del portal de filtraciones en meses anteriores:

> Las muestras de apoyo a WikiLeaks […] han existido, tanto desde Anonymous como desde la empresa de pagos DataCell, que facilitó los pagos para WikiLeaks, sin olvidar al portal *geek alt1040* que inició un boicot de Amazon y PayPal por su acoso a WikiLeaks. Ya antes de la filtración del 28 de noviembre de 2010, el presidente de Veterans for Peace, Mike Ferner, publicó una [*sic*] editorial (julio de 2010) apoyando a WikiLeaks. También el columnista John Pilger escribió un editorial

[167] Véase http://www.freewikileaks.eu.

[168] Ahora el dominio redirige a la página web www.mitnicksecurity.com (último acceso: 10 de septiembre de 2015). Mitnick Security es una compañía fundada por Kevin Mitnick en la que cuenta con el apoyo de un equipo de expertos en seguridad llamado Global Ghost Team.

> en agosto de 2010 en defensa de WikiLeaks, al considerar a éste como "un representante de los intereses de la responsabilidad pública y una nueva forma de periodismo reñida con la dominación y el cinismo [...] Pilger junto al cineasta británico Ken Loach, la multimillonaria británica Jemima Khan y otras celebridades, se ofrecieron a pagar una fianza millonaria que el juez impuso a Assange para que saliera en libertad condicional. El también cineasta y documentalista norteamericano Michael Moore aportó 20.000 dólares a la fianza de Assange, y se puso a disposición de WikiLeaks. También el Premio Nobel de biología en 2002, John Sulston, avaló la fianza (Sánchez Hernández, 2011).

También el expresidente brasileño Lula da Silva defendió a WikiLeaks citándolo como símbolo de la libertad de expresión y aseverando que la detención de Julian Assange atentaba precisamente contra la libertad de expresión (Arias, 2010). De esta manera, el mandatario brasileño identificaba a Assange como una suprema personificación de la libertad de expresión.

El apoyo a Julian Assange por parte del grupo hacktivista Anonymous ha sido también fundamental en esta *wikistory*, hasta el punto de convertir al editor de WikiLeaks en un icono global para las redes hacktivistas: "Todo un movimiento mundial de hackers ve en él a su líder intelectual y está dispuesto a defenderlo. […] La primera guerra virtual ya se ha librado y ha sido en nombre de Julian Assange" (Villeda Saldaña, 2011: 60).

A lo largo de 2010 se puso en marcha lo que los hacktivistas denominaron una guerra digital global que bautizaron como *Operation Payback*. Esta operación desarrollada en la Red consistió en un conjunto de ataques coordinados contra los defensores del *copyright* y del acuerdo multilateral ACTA (Anti-Counterfeiting Trade Agreement) que se estaba gestando para proteger la propiedad intelectual. El 6 de diciembre de 2010, *Operation Payback* se transformó en *Operation Avenge Assange* en defensa de WikiLeaks y de su fundador. Se iniciaba así una serie de ataques globales y en red contra quienes, de una forma u otra, estaban acosando y ahogando económica, política y judicialmente a WikiLeaks.

Como parte de estas acciones organizadas en defensa de Assange y de WikiLeaks también se creó el sitio web Justice For Assange (justice4assange.com), auspiciado por un comité de defensa denominado Julian Assange Defence Fund's (JADF) Committee to Defend Julian Assange, para informar sobre el proceso judicial al líder de WikiLeaks, poner en marcha una campaña a su favor y crear un fondo para su

defensa legal administrado por la firma de contabilidad Hazlems Fenton LLP y el despacho de abogados Finers Stephens Innocent, ambos sitos en Londres.

Estamos en la versión del Assange héroe. Pero Žižek da un giro a esta historia y convierte al héroe en un supremo villano, a la postre, (anti)héroe de la verdad en una sociedad de mascaradas donde nada es lo que parece en las estructuras de poder, sustentadas en la mentira para mantener el orden social:

> En uno de los cables diplomáticos publicados por WikiLeaks, Putin y Medvedev son comparados con Batman y Robin. Es una analogía útil: ¿no es Julian Assange […] un homólogo en la vida real del Joker de la película de Christopher Nolan *The Dark Knight*? En la película, el fiscal de distrito, Harvey Dent, un vigilante obsesivo que es corrompido y comete crímenes, es asesinado por Batman. Batman y su amigo el comisario de policía Gordon se dan cuenta de que la moral de la ciudad se vería afectada si los asesinatos de Dent se hicieran públicos, por lo que traman preservar su imagen haciendo responsable a Batman de los asesinatos. La moraleja de la película es que la mentira es necesaria para mantener la moral pública: sólo una mentira nos puede redimir. No es de extrañar que la única figura de la verdad en la película sea el Joker, el villano supremo. Él deja claro que sus ataques a la ciudad de Gotham se detendrán cuando Batman se quite la máscara y revele su verdadera identidad; para evitar esta revelación y proteger a Batman, Dent dice a la prensa que él es Batman, otra mentira. Con el fin de atrapar al Joker, Gordon finge su propia muerte, otra mentira. El Joker quiere revelar la verdad detrás de la máscara, convencido de que esto va a destruir el orden social (Žižek, 2011: 9).

Sin embargo, la máscara puede adquirir un significado simbólico totalmente diferente, resignificada como protectora de la libertad, como veremos ahora en el caso de los Anonymous.

IV.6.3.1. Anonymous: el anonimato emancipador

Los llamados Anonymous ocupan un lugar central en la corta pero intensa historia del hacktivismo y de WikiLeaks. Representan, como pocos, el poder transformador de la cultura participativa y de la inteligencia colectiva en la sociedad red. Anonymous no es nadie y podemos ser todos. Es una mente colectiva.

IV.6.3.1.1. El anonimato como apología de la libertad en un régimen de sospechas

En un régimen de suspicacias vigorizado por un clima generalizado de inseguridad pocos son tan o más sospechosos de ser una amenaza como aquéllos que se

amparan en el anonimato para ejercer su libertad individual, aunque ésta se ejerza en base a unos principios éticos. En un régimen de desconfianza el anonimato libre se considera potencialmente peligroso. En un régimen de presunción ya no hay culpa verificable, sino imputación por sospecha; ya no hay individuos culpables e inocentes, sino sujetos potencialmente peligrosos y otros inofensivos por su gobernabilidad.

En la era de la sociedad red, el principio de seguridad ha entrado en colisión con el de la libertad como nunca antes. Limitaciones a la libertad del individuo se imponen como necesarias para preservar la seguridad nacional. El sistema de vigilancia panóptico se dilata por las redes de comunicación electrónicas para la defensa e invulnerabilidad del Estado-nación. En este panoptismo construido sobre una base de sospechas y temores, la vigilancia sobre los individuos no se ejerce al nivel de lo que se *hace*, sino de lo que se puede *hacer* o se *es* (Foucault, 1996: 118), o más precisamente, en el panoptismo ciberespacial, de lo que no se *es*. En nuestra sociedad contemporánea, la identidad nos es asignada por registros civiles, documentos nacionales de identidad, expedientes académicos, números de la Seguridad Social, tarjetas de crédito, carnés de conducir, contratos de trabajo, contratos de compra, domicilios, registros telefónicos, etc. Todo ello —nombre, edad, rostros, ubicación, formación, dedicación, consumo, estatus, movilidad y comunicación— son los rasgos que nos hacen reconocibles, localizables, comprensibles y penetrables. Vertidos en un espacio común global y abierto como es el ciberespacio, nos hacen más vulnerables. Pero si no se *es*, si se *existe* en el ciberespacio sin *ser*, o si nuestro *ser* puede revelarse de forma selectiva, la libertad es plena, los riesgos de vulnerabilidad, mínimos y la seguridad para el individuo, máxima.

La privacidad y el anonimato son, para los hackers y libertarios del ciberespacio, la manera de esquivar los mecanismos de control y vigilancia del Estado-nación y de evitar la monitorización de nuestra vida digital por parte de las corporaciones tecnológicas.

La imposibilidad para el poder político y corporativo de encontrar una respuesta a su pregunta "¿quién eres?" es lo que sitúa a los *anónimos* en el resbaladizo y ambiguo terreno de los peligros potenciales para la seguridad del propio Estado-nación y la estabilidad del capitalismo tecnológico. Su máxima expresión se manifiesta en Anonymous.

Los hacktivistas que actúan como Anonymous han maximizado el poder del anonimato en el ciberespacio. Su propio nombre es una apología de la libertad que el anonimato proporciona al individuo en un ecosistema de vigilancia y control.

Anonymous es una amorfa entidad compuesta por un sinnúmero de activistas no identificados que se agrupan periódicamente tanto en el ciberespacio como en las calles. Su uso comunal de *Anonymous* como sustantivo total les proporciona una autodefinición de su identidad colectiva que hace hincapié en la capacidad de poder que perciben de sí mismos en términos de su ubicuidad y anonimato, y articula su creencia de que sus ideas y sus acciones pueden contribuir de manera decisiva a la transformación de la sociedad. Así lo explicitan en uno de sus foros en Internet:

> Somos un conjunto de individuos unidos por ideas. Usted probablemente conoce Anoymous, aunque no sabe exactamente quiénes somos. Somos sus hermanos y hermanas, sus padres e hijos, sus superiores y sus subordinados. Somos los ciudadanos preocupados que estamos a su lado. Anonymous está en todas partes, pero en ninguna parte. Nuestra fuerza reside en nuestra suma. Nuestra voluntad como un todo es el conjunto de voluntades individuales. Nuestra mayor ventaja es el conocimiento de los fundamentos que compartimos como seres humanos. Este conocimiento es fruto de nuestro anonimato.
>
> […] Somos Anonymous. Usted puede ser Anonymous también. Juntos podemos moldear la sociedad. (Why We Protest [Italian Edition!], 2008).

IV.6.3.1.2. Orígenes de Anonymous

Anonymous empezó a operar en el año 2008 y logró notoriedad mundial especialmente cuando sumó fuerzas con WikiLeaks, tras la detención de Julian Assange en diciembre de 2010. Sus acciones se ejectutan principalmente contra la censura y en defensa de la transparencia y la libertad de expresión e información, pero también de cualquier derecho humano individual o colectivo que pueda ser socavado, en el ciberespacio o en la vida *real*. Su objetivo final es devolver el poder al pueblo.

Su estrategia es híbrida, transversal y transmediática: combinan el uso de la computación para la protesta ciberespacial con la manifestación pública en las calles, utilizan canales IRC para interactuar entre ellos y organizarse, y usan los medios sociales en línea como canales de contrainformación de distintos subgrupos y sensibilidades en los que que tienen cabida desde las más radicales protestas políticas hasta las más bellas expresiones artísticas. Sus raíces históricas se hallan en grupos

como Cult of the Dead Cow y Electronic Disturbance Theater. Su lema: "Somos legión. No perdonamos. No olvidamos". Una legión en la que se abrazan hackers, ciberactivistas y activistas.

Anonymous representa el hacktivismo más radical y mediático. Son, en palabras de la antropóloga Gabriella Coleman, "los chicos malos del activismo", representantes de una "libertad caótica" en la que no hay líderes, sino una voz que es la de todos; una voz coral política que surge del encuentro de personas de todas partes del mundo y de todos los estratos sociales y que demanda que "sean los gobiernos quienes teman a los ciudadanos y no al revés" (Coleman, en Knappenberger, 2012).

Por sus acciones en el ciberespacio y en las calles, los Anonymous han sido descritos por las autoridades y por los medios de comunicación convencionales como antipatriotas, niñatos, ciberacosadores, vándalos y simpatizantes del terrorismo (Knappenberger, 2012). Esta criminalización surge de la frustración que causan los golpes políticos de una amorfa entidad formada por un sinnúmero de personas no identificadas. Para desdramatizar esta visión social de los Anonymous, algunos de sus miembros entendieron que debían dar un paso al frente y explicar a cara descubierta lo mismo que han argumentado en el anonimato, para satisfacer así una vieja demanda social que exige la identificación del individuo como paso previo necesario para su legitimación social. Uno de estos Anonymous desvirtualizados es Peter Fein, también miembro del grupo hacktivista Telecomix, dedicado a proveer herramientas y habilidades para la libre expresión e información a disidentes en países con regímenes totalitarios.

Peter Fein decidió salir del anonimato para explicar que Anonymous es "un movimiento político serio" (Knappenberger, 2012) que describe de la siguiente manera: "Anonymous es un cartel, es una bandera que podemos usar. Nos da voz para expresar nuestra oposición a gobiernos y corporaciones que están censurando Internet, algo que muchos ciudadanos demócratas consideran inaceptable" (BBC, 2012).

Fein representa el ala más moderada de los Anonymous. Reconoce que no participa en las acciones ilegales de los miembros más radicales, pero justifica actuaciones como los ataques distribuidos de denegación de servicio: "DDoS es una forma de desobediencia civil, como marchar por las calles o bloquear la entrada de un edificio, lo que a veces es técnicamente ilegal", arguye Fein (BBC, 2012).

Este hacktivista ha colaborado en la organización de protestas de Anonymous, pero su labor se ha centrado principalmente en involucrarse como experto tecnológico en levantamientos civiles en países como Túnez, donde Anonymous prestó soporte a la lucha de hackers y activistas de aquel país contra el régimen de Ben Ali, a finales de 2010 y principios de 2011; en Egipto, colaborando en la reactivación de Internet para los disidentes, tras el apagón comunicativo impuesto por el régimen de Hosni Mubarak durante la revolución iniciada en aquel país en enero de 2011; o en Siria, prestando ayuda técnica a informantes para que pudiesen sortear la censura del Gobierno y proteger sus identidades.

Como sucede con WikiLeaks, son muchas las voces airadas contra Anonymous, pero también las que se alzan en su defensa o intentan comprender sus razones. Una de ellas es la de Steven Levy:

> Bob Dylan escribió una canción que dice «para vivir al margen de la ley tienes que ser honesto». Puede que Anonymous haga algo que no es técnicamente correcto, que tampoco es legalmente correcto, pero lo están haciendo con unos propósitos que para ellos sí son éticos (Levy, en Knappenberger, 2012).

La antropóloga Gabriella Coleman también exalta la cara más comprometida y solidaria de los Anonymous, pero sin obviar las contradicciones de su compleja existencia, manifestadas en acciones por el bien común que chocan con otras éticamente cuestionables o incluso reprobables.

> Los momentos más preocupantes acaecen cuando personas inocentes están atrapadas en el fuego cruzado de Anonymous. Algunos *hacks* me han parecido contraproducentes, y no siempre valen la pena los riesgos asumidos por las personas involucradas. De hecho, partes de Anonymous están plagadas de contradicciones irresolubles (Coleman, 2014: 393)[169].

Richard Stallman también es escéptico respecto a los Anonymous, a quienes sitúa en los límites de la ética hacker:

> Yo no veo esta actitud propia del hacker en Anonymous. Es posible que algunos la tengan, por ejemplo en el desarrollo de algunos programas que usan. Pero la actitud general de los Anonymous no me parece que tenga este espíritu. En todo caso, es difícil afirmar cualquier cosa respecto a todos los Anonymous. Es posible que alguno sí lo tenga (Richard Stallman, en Quian, 2013c).

[169] Todas las citas tomadas de Coleman (2014) son traducciones propias del texto original, en inglés.

Los orígenes de Anonymous se hallan en 4chan, un BBS basado en imágenes que fue lanzado en octubre de 2003 por el empresario tecnológico Christopher 'Moot' Poole, quien por entonces *sólo* era un adolescente anónimo de 15 años que había ideado una red social electrónica libre, sin control, donde los usuarios pueden compartir anónimamente y sin censura imágenes y comentarios en distintos foros temáticos. De estos foros, el identificado como /b/ - Random, de temática libre, fue el caldo de cultivo de Anonymous. Este foro anárquico contribuyó de manera decisiva a la configuración de nuevos patrones culturales sin fronteras para las nuevas generaciones que interpretan y explican el mundo conectados a pantallas y redes electrónicas. En /b/ - Random se han publicado todo tipo de contenidos humorísticos, sarcásticos y grotescos, muchos de éstos considerados por algunos como ofensivos, pero que para otros no han sido más que una apología de la libertad.

En 4chan se halla el origen de la cultura del meme. De hecho, en esta red se originó buena parte de los más famosos memes de Internet; por ejemplo, los memes de gatos que pululan por la Red con tanto éxito, impulsados por el fervor que generan en los usuarios las imágenes de felinos en situaciones graciosas e inverosímiles, y con mensajes ingeniosos, tuvieron su origen en 4chan. Y, en concreto, el foro /b/ fue la principal fuente de esta cultura del meme en Internet que sigue inundando hoy redes sociales como Facebook. Pero también fue un buen caldo de cultivo para los troles de Internet, usuarios que por simple placer publican mensajes provocadores, cáusticos, irrelevantes o fuera de tema en un foro de discusión, un blog, una sala de chat, un medio social o cualquier espacio electrónico abierto a la participación, con el único fin de molestar, ofender, provocar respuestas emocionales en otros usuarios y alterar la conversación para que se convierta en discordia.

Fue en este foro donde, como una suerte de broma o juego, sus usuarios empezaron a identificarse todos como Anonymous —el alias que por defecto se asigna a los usuarios que no adoptan un apodo—, de manera que todos serían uno y uno sería todos. Y como un *todo*, empezaron a trascender sus espacios virtuales para expandirse por la Red y fuera de ella no como organización o grupo, sino como una conciencia global.

Aunque sus primeras acciones estaban salpicadas de chabacanería y carecían de una mínima ética, poco a poco una conciencia social y política se fue apoderando de estos bromistas gamberros y del concepto *Anonymous*. En julio de 2006, la comunidad Anonymous conoció que un niño de dos años con VIH había sido vetado en una piscina de Alabama. Como medida de protesta, usuarios Anonymous de 4chan decidieron registrarse en la página web de Habbo Hotel —una comunidad en línea diseñada para que jóvenes usuarios desarrollen sus propios personajes y experiencias en un hotel virtual— y crearon una multitud de avatares iguales de un personaje negro vestido con un traje gris y pelo al estilo afro con los que bloquearon la entrada a la piscina virtual de Habbo Hotel, disponiéndolos por momentos en forma de esvástica. Los Anonymous declararon el recinto acuático "cerrado por sida". Los Anonymous fueron bloqueados por los administradores de Habbo Hotel y el avatar creado fue borrado, lo que originó denuncias por racismo. Aquella acción fue conocida como la *Great Habbo Raid of '06* e inauguró una serie de intervenciones anuales cada 12 de julio contra Habbo.

Ilustración 27: Avatares creados por Anonymous forman una esvástica en Habbo Hotel.

Fuente: http://habbo.wikia.com/wiki/Lido_Deck (último acceso: 20 de mayo de 2014).

A finales del año 2006, los Anonymous dieron un salto cualitativo cuando decidieron organizarse para atacar a Hal Turner, conocido comentarista radiofónico y bloguero supremacista blanco negador del holocausto judío. Entre diciembre de 2006 y enero de 2007, los Anonymous saturaron el servidor del sitio web de Turner con un ataque DDoS, colapsaron su línea telefónica con cientos de llamadas sarcásticas e incisivas, lo inscribieron en la página web de anuncios clasificados Craiglist como solicitante de servicios de chicas de compañía y pidieron a su nombre un buen número de pizzas y palés industriales que fueron enviados a su domicilio. El objetivo no era sólo incordiar a este apologista del racismo y del nazismo, sino, y sobre todo, minar su economía causándole importantes pérdidas, para reducir así sus transmisiones.

En diciembre de 2007, un pederasta canadiense llamado Chris, Forcand que encontraba a sus víctimas en Internet, fue detenido gracias a los rastreos que los Anonymous habían hecho de este pedófilo. Los hackers de 4chan obtuvieron sus datos personales y se los proporcionaron a la Policía.

La transmutación final de Anonymous se produjo en enero de 2008, cuando finalmente se convirtió en una nueva ánima política hacker. Su primer objetivo fue la Iglesia de la Cienciología. El 14 de enero, una videoentrevista al actor Tom Cruise utilizada como material privado de adoctrinamiento de esta secta fue filtrada a YouTube. El vídeo no tardó en viralizarse en la Red gracias a medios nativos digitales como Gawker. La Iglesia de la Cienciología lo denunció alegando infracción de los derechos de autor. YouTube y otros sitios web cedieron en un principio a las presiones, pero Gawker, que había alojado el vídeo en su servidor, se negó a retirarlo, arguyendo que era de interés informativo. Como respuesta a lo que consideraron un acto de censura, el 16 de enero los Anonymous empezaron a organizar una campaña de protesta en los IRC y BBS en los que actuaban. Sus acciones contra la Iglesia de la Cienciología comenzaron el 18 de enero. Tres días después, los hacktivistas publicaron en un canal abierto en YouTube llamado ChurchOfScientology su primera pieza audiovisual, titulada *Message to Scientology*, editada como un *time-lapse* de grises nubes al que acompaña una voz en *off* sintetizada por computadora que finaliza su arenga contra la censura y la Iglesia de la Cienciología con el lema que ha acompañado a los Anonymous desde entonces: "Somos Anonymous. Somos legión. No olvidamos. No perdonamos. Espéranos". Esta primera campaña transnacional de Anonymous se dio a conocer como *Project Chanology*. Su objetivo: hacer desaparecer la cienciología de Internet.

Ilustración 28: Primer vídeo publicado por Anonymous, el 21 de enero de 2008.

Fuente: captura propia tomada en el canal ChurchOfScientology en YouTube, del vídeo *Message to Scientology*, en https://youtu.be/JCbKv9yiLiQ (última consulta: 19 de mayo de 2014).

Cientos de militantes *anónimos* se unieron a la causa para tumbar las páginas web de la secta con ataques DDoS, inundar de mensajes sus bandejas de correo electrónico, enviar faxes negros para agotar sus recursos de impresión y colapsar sus máquinas, saturar sus líneas telefónicas y, también, protestar en las calles en las que, por primera vez, los Anonymous usaron la máscara de Guy Fawkes.

Tras las primeras ciberacciones contra la Iglesia de la Cienciología, Anonymous siguió publicando más vídeos con la misma fórmula audiovisual, buscando atraer multitudes. El 28 de enero se lanzó el vídeo *Call to Action* para convocar una protesta mundial frente a las sedes de la Iglesia de la Cienciología el 10 de febrero, coincidiendo con el cumpleaños de Lisa McPherson, ciencióloga fallecida cuya familia y amigos atribuyeron su muerte a esta secta. Un tercer vídeo fue publicado el 1 de enero con el título *Code of Conduct*, con veintidós reglas para armar una protesta pacífica y a la vez segura para los manifestantes; la número diecisiete decía:

> Cúbrete la cara. Esto evitará que puedas ser identificado en vídeos tomados por hostiles, otros manifestantes o de seguridad. Usa pañuelos, sombreros y gafas de sol. Las máscaras no son necesarias, y ponérselas en el contexto de una manifestación pública está prohibido en algunas jurisdicciones (ChurchOfScientology, 2008, 1 de febrero).

Sin embargo, a alguien se le ocurrió que una máscara podría ser utilizada para proteger a los Anonymous. Tras el estreno en el año 2006 de la película *V de Vendetta*, la máscara de Guy Fawkes se popularizó enormemente como un producto cultural y originó un meme en 4chan, donde campaban los Anonymous. Allí se había hecho famoso un torpe monigote llamado Epic Fail Guy que no da pie con bola en nada de lo que hace. El 30 de septiembre de 2006, Epic Fail Guy fue dibujado en 4chan recogiendo de un cubo de basura la famosa máscara de Guy Fawkes, el personaje histórico que también falló en su intento de hacer saltar por los aires el Parlamento británico; a partir de entonces, Epic Fail Guy se viralizó por la web con esta máscara y se convirtió en meme.

Ilustración 29: Primera ilustración de Epic Fail Guy con la máscara de *V de Vendetta*.

Fuente: http://knowyourmeme.com/memes/epic-fail-guy (último acceso: 20 de mayo de 2014).

El 10 de febrero de 2008 tuvo lugar la primera protesta mundial organizada por Anonymous en las calles, frente a los centros de la Iglesia de la Cienciología. Se calcula que participaron unas diez mil personas en Estados Unidos, Canadá, Australia, Israel y Europa. Fue también la primera vez que la comunidad Anonymous se *desvirtualizó* (Knappenberger, 2012). Muchos se cubrieron con la máscara de *V de Vendetta*. Los Anonymous querían proteger sus identidades por seguridad personal, pero también pensaron la manera de migrar al mundo físico con el mismo anonimato que en el ciberespacio les significaba como un individuo colectivo. La solución brotó de una curiosa combinación de elementos que habían definido la propia evolución de los Anonymous: la cultura bromista del meme, los mundos fantásticos del cómic y del cine, y la emergente conciencia política colectiva de aquellos jóvenes sin rostro ni identidad.

Ilustración 30: Manifestantes de Anonymous en Londres, el 10 de febrero de 2008.

Autor: Paul Williams. Fuente: Wikipedia.

La máscara de *V de Vendetta* se había hecho famosa en los tablones electrónicos de los Anonymous con el meme Epic Fail Guy y se había convertido en un icono de la cultura popular que se podía comprar por un precio módico casi en cualquier ciudad del mundo donde se estranase la película dirigida por James McTeigue, basada en la novela gráfica de Alan Moore (Coleman, 2014: 64). Además, la famosa escena final del filme, con las multitudes retando con un solo rostro —el de Guy Fawkes— al poder autoritario, era precisamente una representación de lo que Anonymous quería ser (Knappenberger, 2012).

> Anonymous ha tomado un símbolo popularizado por Hollywood y lo ha convertido en revolucionario. Es un excelente ejemplo de la lucha contra la mercantilización, una ocurrencia excepcional (Coleman, 2014: 271).

Aquellas acciones de protesta llevaron a la Iglesia de la Cienciología a planear una campaña de acoso e intimidación en Estados Unidos contra varios Anonymous identificados. Aquelló derivó en redadas del FBI y acusaciones que conllevaban penas de cárcel de hasta cinco años y multas de 100.000 dólares por los ataques DDoS (Knappenberger, 2012). Finalmente, dos Anonymous acabaron entre rejas. Dmitriy Guzner, de 19 años, se convirtió en el primer miembro de esta comunidad hacktivista condenado por un tribunal. En noviembre de 2009 se le impuso una pena de un año de prisión, dos años de libertad condicional y una multa de 37.500 dólares. En mayo de 2010, Brian Thomas Mettenbrink, de 20 años, fue condenado a un año de prisión y otro de libertad vigilada, y se le impuso una multa de 20.000 dólares.

Project Chanology supuso la transfiguración de un subgrupo de la cultura digital en un movimiento político que galvanizó la lucha por los derechos civiles, tras una época de depresión civil marcada por los atentados del 11 de septiembre de 2001 en Estados Unidos. Fue la primera gran campaña de protesta política global híbrida de Anonymous contra la censura en Internet y marcó el inicio de una nueva estrategia hacktivista, con la utilización de los medios sociales de las multitudes en línea como canales de comunicación. De ahí en adelante, Anonymous se convirtió en un fenómeno global vinculado estrechamente a las grandes revoluciones y protestas civiles de los últimos años: la defensa de WikiLeaks, el movimiento *Occupy*, la Primavera Árabe… Y la máscara de Guy Fawkes fue colectivamente resignificada como elemento simbólico de una idea compartida: la libertad.

IV.6.3.1.3. La máscara que a todos libera

Bajo el nombre de Anoymous, una nueva disidencia transnacional se articula para luchar contra las injusticias y por la defensa de una Internet libre. Su arma es el anonimato. Es precisamente ese anonimato deliberado, la imposibilidad de identificar a *alguien*, la opacidad del grupo anónimo que protege la identidad individual y otorga cohesión, solidez y horizontalidad, lo que desconcierta al vigilante de un sistema

autoritario jerárquico. Un anonimato premeditado y robusto que se contrapone con los secretos de Estado y con la falsa individualidad que nos promete la cultura de masas sellándonos con marcas que en apariencia nos singularizan pero que en realidad nos uniformizan, despersonalizan y masifican. El anonimato consciente, deliberado y voluntario es, en esta sociedad del exhibicionismo de las masas, un acto disruptivo que conduce hacia la libertad del individuo.

Al sacrificar el *yo* público, rehuyendo de liderazgos y, sobre todo, al negarse a participar en el *juego* de la autopromoción, Anonymous asegura el misterio; esto en sí mismo es un acto político radical en un orden social basado en la vigilancia ubicua y la celebración de un galopante individualismo y egoísmo (Coleman, 2014: 399).

El paradigma de ese anonimato redentor y emancipador es el misterioso anarquista revolucionario de la novela gráfica y de la película *V de Vendetta* que se esconde bajo el apodo 'V' y se oculta tras la máscara del disidente histórico Guy Fawkes. "Debajo de esta máscara hay más que carne. Debajo de esta máscara hay una idea, Sr. Creedy. Y las ideas son a prueba de balas", dice el protagonista. Es decir, los ideales y grandes relatos que parecían haber sido desterrados en la sociedad posmoderna vuelven a revivir en los individuos bajo una misma máscara, una misma identidad, un *yo* colectivo. Por eso no es casual que los miembros y los partidarios de Anonymous hayan elegido esta máscara popularizada por la película dirigida por James McTeigue, que es la que acompañó también a Assange durante su proceso judicial en Londres, y que él mismo se puso en unas protestas del movimiento *Occupy London*[170] el 15 de octubre de 2011.

Ilustración 31: Assange, en las protestas del movimiento *Occupy London*.

Autor: Mike Kemp. Fuente: http://liberalsarecool.com/post/11495369017/julian-assange-in-guy-fawkes-mask-today-in

[170] *Occupy London* es un movimiento civil contra las desigualdades económicas, las injusticias sociales, la avaricia financiera y empresarial, y las presiones de los *lobbies* al Gobierno británico. Su primera acción de protesta fue el 15 de octubre de 2011. Los activistas intentaron acampar frente a la Bolsa de Londres. Es parte del movimiento global de protestas ciudadanas surgidos por la crisis económica mundial, las políticas neoliberales y los recortes en derechos laborales y sociales, que han tenido otros epicentros, como la Puerta del Sol de Madrid con los *indignados* y el centro financiero de Nueva York con las acciones de *Occupy Wall Street*.

Y tampoco es casual que la película fuera escrita y producida por los hermanos Wachowski, autores de la trilogía cinematográfica *cyberpunk The Matrix*, otra historia que inspira a muchos a reconocer en Julian Assange a Neo, el disidente protagonista de estas películas, un Prometeo hacker (Mosco, 2004: 48).

Si en la interpretación de Žižek (2001), Batman es una más de las caretas de una gran mascarada donde todo parece y nada es lo que aparenta bajo las estructuras de poder tradicionales, sustentadas en la mentira y en el engaño para mantener el orden social, en el mundo de WikiLeaks y del hacktivismo, la máscara —una máscara— ha adquirido un poder simbólico sustancial de movilización y de subversión social: la máscara de un hombre, de un héroe reconocible en todos y en nadie; la máscara del disidente, bajo la que se resguarda y se une una legión de hacktivistas y simpatizantes de Julian Assange y de WikiLeaks. Es la máscara protectora e identitaria de la libertad, un icono popular de la lucha contra la tiranía de la mascarada del sistema político y financiero mundial. Guy Fawkes contra Batman; el disidente contra el guardián del orden tradicional; la cara unívoca de la libertad del individuo frente al baile de caretas de la mentira social masificada. La máscara de Fawkes, en definitiva, cumple una doble función social: identificación colectiva (refuerzo del *yo* colectivo) y anonimato simultáneo (garante de la libertad del *yo* individuo).

La máscara de Guy Fawkes es ahora también logo resignificado en las redes en línea y portado en el mundo físico; un logo legible, escalable, reproducible, distinguible, memorable y adaptable, que adquiere la fuerza de la ubicuidad con la que operan los logotipos como "lo más parecido que tenemos a un idioma internacional", reconocidos y comprendidos casi en cualquier parte del mundo, independientemente del idioma que allí se hable y escriba (Klein, 2001: 27).

David Lloyd, dibujante británico autor de la imagen original de la máscara de Guy Fawkes para la novela gráfica de Alan Moore, entiende la función simbólica que ha adquirido el rostro plastificado de Guy Fawkes. En unas declaraciones recogidas por la BBC el 20 de octubre de 2011, cinco días después de las manifestaciones del movimiento *Occupy London*, Lloyd explica: "Mi impresión es que Anonymous necesitaba una imagen polivalente que les sirviera tanto para ocultar su identidad como para simbolizar que defienden el individualismo. V de Vendetta es una historia sobre alguien solo contra el sistema" (Waites, 2011).

El héroe anarquista ya no está solo. El director James McTeigue introdujo un giro en la historia adaptada al cine (2006), introduciendo una escena final en la que una multitud de ciudadanos cubiertos con la máscara de Guy Fawkes toma las calles para respaldar al héroe que sacrificó su vida por acabar con el Estado opresor. Guy Fawkes no está solo, al menos en su resucitada versión del siglo XXI encarnada por Julian Assange y su legión de seguidores.

Es importante además recordar aquí la importancia que Assange siempre le ha dado a la máscara como garante de la verdad. Como ya hemos mencionado anterioremente, la deificada obra de Dreyfus y Assange, *Underground* (1997), arranca con este aforismo de Oscar Wilde: "El hombre es menos uno mismo cuando habla en primera persona. Dale una máscara y te dirá la verdad". Pero no se puede obviar que la elección de Assange como rostro reconocible de un movimiento transnacional de hacktisvistas es también la elección del mártir disidente, del ser humano que soportará sobre sus hombros la pesada *cruz* para salvar a la humanidad y que servirá de fuente inspiradora y guía en la *salvación*. El fundador de WikiLeaks simboliza la fuerza disruptiva del disidente y su emancipación subversiva.

IV.6.4. El antagonista: Mark Zuckerberg

Todo héroe necesita un villano para explicar su razón de ser y de existir. La necesidad de personificar el mal, de ofrecer un rostro y un nombre, también existe en la versión que propone a Julian Assange como héroe. Si los Anonymous y todo el nuevo movimiento civil líquido y cibernético necesitaban un icono de carne y hueso (Muñoz-Rojas, 2011), a su vez el héroe necesitaba poner rostro a su enemigo. Julian Assange necesitaba un enemigo de carne y hueso que personificara el poder del Estado-nación y del Estado-corporativo. Y qué mejor antagonista que Mark Zuckerberg, presidente del que muchos consideran la mayor *nación* del mundo por número de *habitantes*: Facebook[171]. Esto ha facilitado la estrategia de Assange para desacreditar a Zuckerberg como gobernante del primer Estado-nación líquido, el mayor aparato de control y vigilancia jamás creado —según el propio Assange—, cooperante necesario de los

[171] Facebook alcanzó en la primavera de 2015 los 1.440 millones de usuarios activos, casi cien millones más que la población de China, el país más populoso del mundo, con 1.360 millones de habitantes. Véase: Mathew, J. (2015, 23 de abril): 'Facebook is now more 'populous' than China with 1.44 billion monthly active users'. *International Business Times*. Disponible en: <http://www.ibtimes.co.uk/facebook-now-more-populous-china-1-44-billion-monthly-active-users-1497909> (último acceso, 25 de abril de 2015).

Estados-nación tradicionales y de las corporaciones empresariales, a los que sirve en bandeja nuestro *ADN* virtual.

La revista *Time* contribuyó a este enfrentamiento cuando nombró a Zuckerberg "Personaje del Año" el 15 de diciembre de 2010, en pleno apogeo del fenómeno WikiLeaks tras la publicación de los cables diplomáticos de Estados Unidos. Assange había sido el más votado por los lectores de la revista, con 382.020 de 1.249.425 votos totales emitidos (Friedman, 2010) y había sido portada de *Time* sólo dos días antes, en una metáfora visual poderosa: una fotografía acromática (en blanco y negro) de Assange y su boca tapada por el cromatismo de la bandera de Estados Unidos; una imagen a la que acompañaba el título 'Do You Want to Know a Secret?' Sin embargo, los editores de la revista decidieron anular el voto popular y nombraron a Zuckerberg "persona del año", pese a que había sido el décimo más votado, por detrás de Assange, el entonces primer ministro turco Recep Tayyip Erdogan, la cantante Lady Gaga, los cómicos Jon Stewart y Stephen Colbert, el comentarista político conservador Glenn Beck, el presidente Barack Obama, Steve Jobs, los mineros de Chile rescatados de la mina de San José y los desempleados estadounidenses.

Ilustración 32: Portadas de la revista *Time* dedicadas a Julian Assange y Mark Zuckerberg.

Fuente: *Time*.

Assange colaboró en la creación de su antagonista. "Facebook es la mayor máquina de espionaje jamás inventada", sentenció en una entrevista en RT en la que vinculó a Facebook con el Servicio Secreto de Estados Unidos: "Todo el mundo debería

entender que cuando añade un amigo en Facebook está trabajando gratis para la Agencia de Inteligencia de Estados Unidos, y ayuda a crear una base de datos para ellos", advirtió un agorero Assange en aquella entrevista (Emmett, 2011). Pero para ser precisos, el fundador de WikiLeaks no acusa a la CIA de administrar directamente Facebook, sino de ejercer presión legal y política sobre esta compañía y sobre otras grandes corporaciones tecnológicas que almacenan datos e información de cientos de millones de personas de todo el mundo; una capacidad que permite a esta agencia de inteligencia meter mano a estas empresas, como se ha demostrado con las revelaciones de documentos secretos de Edward Snowden sobre los programas de vigilancia y espionaje estadounidenses.

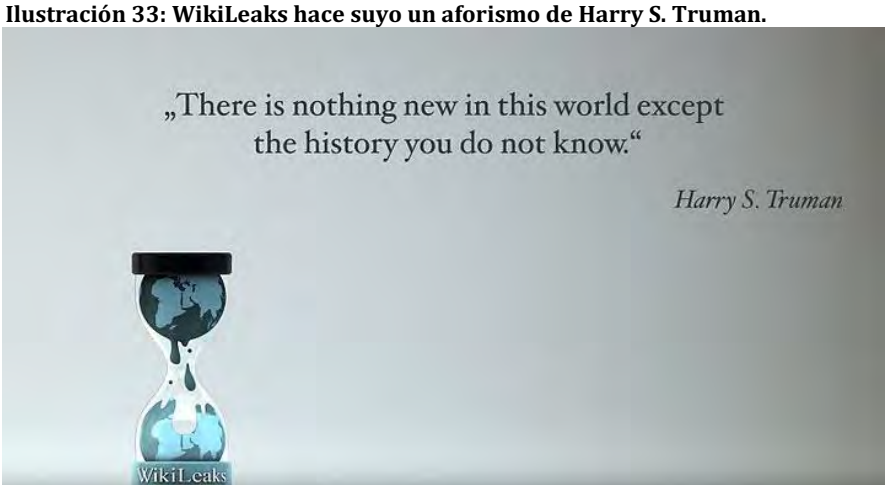
Lo cierto es que la idea de Facebook como un aparato de vigilancia global se ha extendido entre la comunidad hacker. Stallman reconoce que no usa las redes sociales por las amenazas que entrañan para la privacidad de los individuos, especialmente Facebook:

> No las uso [las redes sociales] porque, primero, sería incómodo para mí y, segundo, porque en algunos casos son abusivas con los usuarios, como por ejemplo Facebook, que es un sistema para espiar a la gente. Yo le digo a todo el mundo que no ponga mis fotos en Facebook (Richard Stallman, en Quian, 2013c).

Sin embargo, en el caso de WikiLeaks se produce una paradoja: Assange señala los peligros de Facebook, pero WikiLeaks tiene una cuenta activa en esta red social donde, por ejemplo, el 29 de enero de 2011 inició una campaña para que sus seguidores apoyasen la difusión de los cables filtrados que desnudan la política exterior de Estados Unidos. Para ello, WkiLeaks invitó a sus seguidores en Facebook a usar el servicio Twittbon, que permite crear campañas para que los usuarios se adhieran a una causa mediante la inserción automática de una pequeña imagen en el avatar de sus cuentas en Facebook y Twitter. Otra paradoja: entre los 26 *wallpapers* que WikiLeaks comparte en su página de Facebook, en uno de ellos se recoge un famoso aforismo del trigésimo tercer presidente de Estados Unidos, Harry S. Truman: "There is nothing new in the world except the history you do not know". WikiLeaks toma como mensaje esta reveladora y oportuna sentencia del presidente que ordenó lanzar las bombas atómicas sobre Hiroshima y Nagasaki y la creación de la CIA, templo de los documentos secretos, la agencia para la que algunos dicen que trabaja Assange y a la que otros

acusan de organizar la persecución del líder de WikiLeaks e incluso de buscar su asesinato.

Ilustración 33: WikiLeaks hace suyo un aforismo de Harry S. Truman.



Fuente: Página de WikiLeaks en Facebook (https://www.facebook.com/wikileaks/).

IV.6.5. De Manning a Snowden: los nuevos mártires de la libertad de expresión

Como ya hemos explicado, en WikiLeaks es tan importante el código informático como el código emocional, con el que apela a la conciencia de los individuos que trabajan en el centro neurálgico del poder para que filtren los secretos a los que tienen acceso como operarios del sistema.

> El principal gancho […] de WikiLeaks fue que inspiró a gente a proporcionar documentos importantes para el bien común, para la humanidad, información que debe ser de dominio público. Y que pudieran garantizar que la fuente no pudiese ser rastreada. […] Ese fue también el caso de Manning: no fue a través del proceso tecnológico de WikiLeaks o del proceso de interacción humana por lo que esa fuente fue comprometida (Christensen y Jónsdóttir, 2014: 2563)[172].

Domscheit-Berg, excolaborador de Julian Assange, defiende los procesos de WikiLeaks para proteger a sus confidentes:

> Nosotros no podíamos ni queríamos saber quiénes eran nuestras fuentes, eso formaba parte del concepto de seguridad […] Su protección era nuestra mayor prioridad (Domscheit-Berg, 2011: 151).

[172] Traducción propia del texto original, en inglés.

Braman aporta a este asunto:

> La configuración del anonimato de WikiLeaks fue diseñada por Julian Assange, y debe mucho a su habilidad para programar. Funciona tan bien, según él, que ni él mismo tiene manera de saber si Bradley Manning fue en realidad la fuente de los materiales del *Cablegate* (Braman, 2014: 2609).

En el caso de Manning, lo que falló no fueron ni los protocolos ni los procesos tecnológicos de WikiLeaks, sino el factor humano. Manning había confesado a un exhacker, vía chat, que él era el responsable de las filtraciones a WikiLeaks de documentos secretos de Estados Unidos. El exhacker en cuestión era Adrian Lamo, quien decidió delatar a Manning por filtrar el vídeo de *Collateral Murder*, documentos secretos de las guerras en Afganistán e Irak, y cables diplomáticos estadounidenses. Lamo justificó su denuncia alegando que aquellas filtraciones ponían en riesgo vidas. Sin embargo, "no hay evidencias de que nadie haya muerto como resultado de la información filtrada" (chelseamanning.org).

¿Por qué Manning le confesó su secreto? Lamo se había ganado la confianza de Manning, quien le admiraba por haber sido un hacker famoso que ya había tenido encontronazos con el FBI y la justicia por sus actividades informáticas, especialmente por haber penetrado en la red informática de *The New York Times*, modificar sus bases de datos y añadir su nombre a la lista de columnistas del periódico. Por lo tanto, Manning fue traicionado por un confidente ajeno a WikiLeaks. El factor humano había causado el fallo en el sistema de filtraciones: "Por primera vez comprendimos las deficiencias sociales de nuestro proyecto" (Domscheit-Berg, 2011: 151).

Tras la detención de Manning en Bagdad, en mayo de 2010, WikiLeaks le ofreció soporte económico y legal —a través de la Fundación Wau Holland—, pero también apoyo social mediante la movilización de la opinión pública. El exsoldado y analista de inteligencia del Ejército estadounidense Bradley Edward Manning —ahora Chelsea Elizabeth Manning[173]— se enfrentó a una pena máxima de noventa años en prisión por veinte de los veintidós delitos por los que fue declarado culpable el 30 de julio de 2013, entre ellos, seis por violación de la Ley de Espionaje, además de robo de información gubernamental, fraude informático y abuso de su posición como analista en

[173] Manning se confesó públicamente transexual el 22 de agosto de 2013, inició un tratamiento hormonal para culminar su feminidad y cambió su nombre por el de Chelsea Elizabeth Manning.

Irak, entre otros cargos. Afortunadamente para el exsoldado, el fiscal no consiguió que fuese encontrado culpable del más grave de los veintidós delitos que se le habían imputabdo, el de ayuda al enemigo, que le hubiese acarreado una pena de cadena perpetua, o incluso de muerte. La Fiscalía buscó una pena mínima de sesenta años de cárcel que sirviera de ejemplo disuasorio; la defensa de Manning esperaba que la pena máxima fuese de veinticinco años, el periodo que debe pasar para que documentos secretos puedan hacerse públicos (Saiz, 2013). Finalmente, fue condenado el 21 de agosto de 2013 a treinta y cinco años de cárcel, a los que se restarían los 1.294 días que estuvo en prisión preventiva, primero en el Campamento Arifijan, en Kuwait, y luego en la prisión militar de la base de Quantico, en el estado de Virgina, donde estuvo los nueve primeros meses totalmente aislado, en unas condiciones descritas como inhumanas, crueles e incluso de tortura (Greenwald, 2010).

La sentencia fue recibida en las redes de apoyo a Manning como "excepcionalmente dura por un delito no violento" (Chelsea Manning Support Network). La condena se consideró más injusta cuando se comparó con otras sentencias dictadas contra personal militar de Estados Unidos involucrado en asesinatos y torturas: la del teniente primero Michael Behenna, condenado a veinticinco años de prisión —finalmente rebajados a quince— por matar a un ciudadano iraquí desarmado que estaba siendo interrogado sobre supuestas actividades terroristas; la del cabo Jeremy Morlock, uno de los soldados que reconoció haber participado en matanzas indiscriminadas de civiles en Afganistan en 2010, condenado a veinticuatro años de cárcel; o las de los soldados acusados de tratos vejatorios y torturas a presos iraquíes en la cárcel de Abu Ghraib, entre los cuales la mayor condena, de diez años de prisión, fue para el suboficial Charles Graner.

The New York Times, en un editorial publicado el mismo día que se dictó sentencia, consideró excesiva la pena impuesta a Manning:

> […] 35 años es una condenada demasiado larga, se mire por donde se mire. En las más de dos semanas de audiencias, los abogados del Gobierno hicieron afirmaciones vagas y en gran parte especulativas de que las filtraciones del soldado Manning habían puesto en peligro vidas y «enfriado» relaciones diplomáticas. Por otro lado, gran parte de lo que el soldado Manning liberó era de valor público […] (*The New York Times*, 2013)[174].

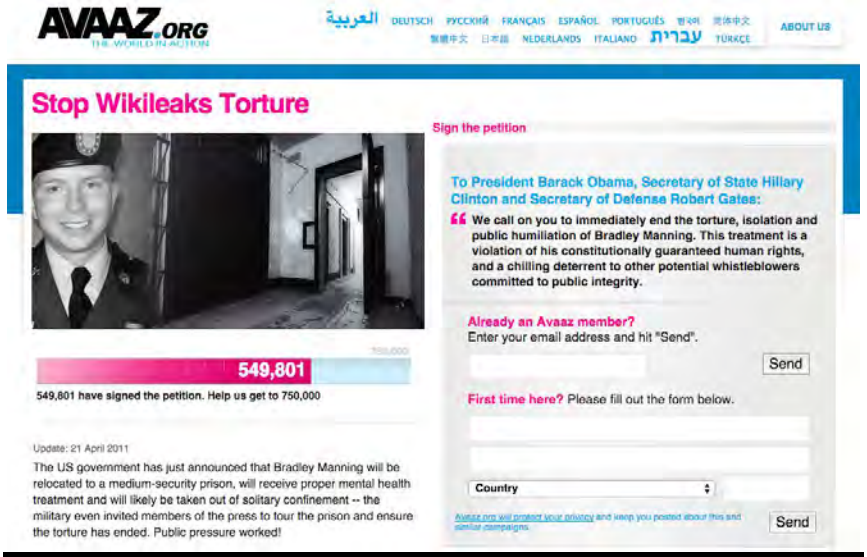
[174] Traducción propia del texto original, en inglés.

Dos años antes, el periódico neoyorkino ya había denunciado en otro editorial los "abusos al soldado Manning" (*The New York Times*, 2011). La American Civil Liberties Union también denunció en un comunicado:

> Cuando a un soldado que ha compartido información con la prensa se le impone un castigo mayor que a otros que han torturado o asesinado a civiles, es que algo funciona extremadamente mal en nuestro sistema de justicia (Saiz, 2013).

Otras organizaciones civiles internacionales, como Amnistía Internacional, Human Rights Watch o Avaaz, también intercedieron por Manning y pidieron para él un trato digno y un juicio justo. Por ejemplo, en abril de 2011, Avaaz recogió en su plataforma en línea 549.801 firmas virtuales para pedir al presidente Barack Obama, a la secretaria de Estado, Hillary Clinton, y al secretario de Defensa, Robert Gates, que acabasen con el aislamiento de Manning y con las humillaciones y abusos documentados a los que estaba siendo sometido, confinado en una celda de apenas dos por cuatro metros, sin ventana, de la que sólo se le permitía salir una hora al día, y sometido a una constante vigilancia por parte de sus guardianes para que no pudiese ni siquiera hacer ejercicios físicos, durmiendo sin almohada ni sábanas, en alguna ocasión incluso totalmente desnudo. (Logan, 2011).

Ilustración 34: Campaña a favor de Manning en Avaaz.org.



Fuente: captura de pantalla propia tomada de http://avaaz.org/en/bradley_manning/.

Previamente, en marzo de 2011, doscientos noventa y cinco juristas firmaron una declaración para denunciar la "humillación y maltrato al soldado Bradley Manning", sometido a "condiciones denigrantes e inhumanas que son ilegales e inmorales", y que constituyen una violación de las garantías de la Quinta Enmienda a la Constitución de Estados Unidos contra el castigo sin juicio, y de la Octava Enmienda, que prohibe al Gobierno imponer castigos crueles e inusuales (Ackerman, 2011). Esta declaración fue encabezada por Bruce Ackerman —profesor Sterling en la Yale Law School— y Yochai Benkler —profesor de Harvard y codirector del Berkman Center for Internet and Society de esta universidad—, y fue firmada, entre otros, por el profesor Laurence H. Tribe, de la Harvard University —quien impartió clases a Barack Obama y fue asesor del Departamento de Justicia— y Jack Balkin, profesor de la Yale Law School, fundador del centro de estudio e investigación Information Society Project de Yale y creador del blog colaborativo sobre Derecho *Balkinization*.

La lista de personalidades y activistas que se han sumado a las campañas en apoyo a Manning es vasta e incluye, entre otros, al exanalista Daniel Ellsberg —el hombre que filtró los *Papeles del Pentágono* sobre la guerra en Vietnam—, el profesor Noam Chomsky, el excongresista republicano Ron Paul, el congresista demócrata Dennis Kucinich, la periodista e investigadora Naomi Klein, el cineasta Michael Moore, Rick Falkvinge —fundador del Partido Pirata sueco—, el bloguero y activista tunecino Slim Amamou, el exoficial estadounidense y combatiente en Irak Daniel Choi, la actriz Roseanne Barr —quien militó primero en el Partido Verde de Estados Unidos y luego fue candidata a la Presidencia de su país por el Peace and Freedom Party—, Jill Stein —candidata presidencial del Partido Verde—, la activista política Medea Benjamin —cofundadora de las ONG Code Pink: Women for Peace y Global Exchange—, el activista y exmarine Scott Olsen —miembro de la organización Iraq Veterans Against the War y del movimiento *Occupy Oakland*—, la activista Annie Leonard —reconocida experta en responsabilidad social corporativa, desarrollo sostenible, riesgos laborales, cooperación internacional y salud, y autora del cortometraje documental animado *The Story of Stuff* (2007)—, el activista británico de los derechos humanos Peter Tatchell, el guitarrista Tom Morello —miembro de Rage Against the Machine, Audioslave, The Nightwatchmen—, Jeff Paterson —director del proyecto Courage to Resist, quien en agosto de 1990 se convirtió en el primero de muchos militares estadounidenses en negarse a combatir en Irak—, el rapero Mutulu Olugbala —también conocido por su

nombre artístico M-1 y mitad del dúo Dead Prez—, o el músico y cantante Graham Nash —célebre por ser parte del grupo Crosby, Stills, Nash & Young—, quien contribuyó a la causa de Manning con la canción *Almost Gone (The Ballad of Bradley Manning)*[175], escrita junto con James Raymond (hijo de David Crosby).

La presión social motivó el traslado de Manning, el 21 de abril de 2011, de Quantico a Fort Leavenworth (Kansas), donde fue considerado preso de bajo riesgo y sus condiciones de confinamiento, mejoradas (Chelsea Manning Support Network).

La campaña más importante a favor de Manning se ha articulado en el sitio web ChelseaManning.org —anteriormente, BradleyManning.org—, en colaboración con la organización Courage to Resist, que ha estado gestionando el fondo para su defensa legal. Esta red en apoyo a Manning cuenta con un consejo asesor compuesto por: Medea Benjamin (Code Pink: Women for Peace), Marsha Coleman-Adebayo (National Whistleblower Center), Daniel Ellsberg (responsable de la filtración de los *Papeles del Pentágono*), Kathleen Gilberd (The Military Law Task Force of the National Lawyers Guild), el exsenador demócrata Mike Gravel, Kimber Heinz (War Resisters League), la parlamanentaria islandesa Birgitta Jónsdóttir, el exanalista de la CIA y activista Ray McGovern, el cineasta Michael Moore, la coronel retirada Ann Wright y Jose Vasquez (Iraq Veterans against the War).

---

175 La canción fue compuesta en primavera de 2011 y publicada en diciembre de ese año. Se ofreció en descarga directa y gratuita en las páginas web www.grahamnash.com y www.bradleymanning.org. Andrew Thomas realizó el videoclip de este tema, accesible en YouTube en la URL https://youtu.be/dAYG7yJpBbQ (último acceso: 30 de septiembre de 2015). Esta es la letra de la canción:

Locked up in a white room, underneath a glaring light
Every 5 minutes, they're asking me if I'm alright
Locked up in a white room naked as the day I was born
24 bright light, 24 all alone
What I did was show some truth to the working man
What I did was blow the whistle and the games began
Tell the truth and it will set you free
That's what they taught me as a child
But I can't be silent after all I've seen and done
24 bright light I'm almost gone, almost gone
Locked up in a white room, dying to communicate
Trying to hang in there underneath a crushing wait
Locked up in a white room I'm always facing time
24 bright light, 24 down the line
What I did was show some truth to the working man
What I did was blow the whistle and the games began
But I did my duty to my country first
That's what they taught me as a man
But I can't be silent after all I've seen and done
24 bright light I'm almost gone, almost gone
(Treat me like a human, Treat me like a man).

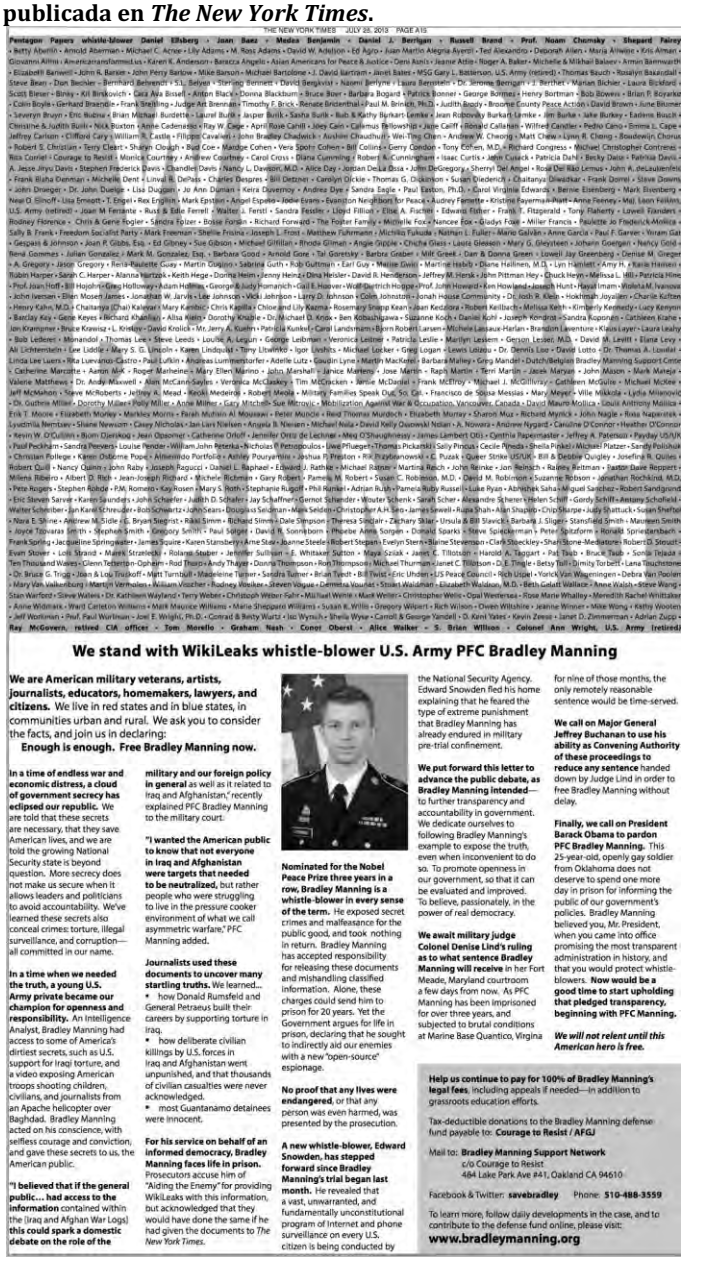
Ilustración 35: Sitio web para la defensa del soldado Manning.

Fuente: captura de pantalla propia tomada de https://www.chelseamanning.org/.

Los miembros de esta red de apoyo a Manning han advertido de las perniciosas consecuencias para la libertad de expresión y de información derivadas de este proceso: "Este caso sienta un precedente peligroso para la Primera Enmienda [a la Constitución de Estados Unidos], exponiendo a los denunciantes y a quienes les ayudan a una persecución extrema" (Chelsea Manning Support Network).

El 25 de julio de 2013, estos partidarios de WikiLeaks y de Manning publicaron un anuncio a toda página en *The New York Times*, con un coste de 52.000 dólares, que incluía un gran titular, "We Are Bradley Manning", los nombres de los firmantes impresos de fondo y una carta suscrita por ochocientos cincuenta "militares veteranos, artistas, periodistas, educadores, amas de casa, abogados y ciudadanos" que viven en "estados rojos [demócratas] y azules [republicanos], en comunidades urbanas y rurales", y que se ensalzan a Manning como un héroe de la libertad (Chelsea Manning Support Network, 2013).

Ilustración 36: Campaña a favor del soldado Manning publicada en *The New York Times*.



THE NEW YORK TIMES · JULY 26, 2013 · PAGE A15

We stand with WikiLeaks whistle-blower U.S. Army PFC Bradley Manning

We are American military veterans, artists, journalists, educators, homemakers, lawyers, and citizens. We live in red states and in blue states, in communities urban and rural. We ask you to consider the facts, and join us in declaring:

Enough is enough. Free Bradley Manning now.

In a time of endless war and economic distress, a cloud of government secrecy has eclipsed our republic. We are told that these secrets are necessary, that they save American lives, and we are told the growing National Security state is beyond question. More secrecy does not make us secure when it allows leaders and politicians to avoid accountability. We've learned these secrets also conceal crimes: torture, illegal surveillance, and corruption—all committed in our name.

In a time when we needed the truth, a young U.S. Army private became our champion for openness and responsibility. An Intelligence Analyst, Bradley Manning had access to some of America's dirtiest secrets, such as U.S. support for Iraqi torture, and a video exposing American troops shooting children, civilians, and journalists from an Apache helicopter over Baghdad. Bradley Manning acted on his conscience, with selfless courage and conviction, and gave these secrets to us, the American public.

"I believed that if the general public… had access to the information contained within the [Iraq and Afghan War Logs] **this could spark a domestic debate on the role of the military and our foreign policy in general** as well as it related to Iraq and Afghanistan," recently explained PFC Bradley Manning to the military court.

"I wanted the American public to know that not everyone in Iraq and Afghanistan were targets that needed to be neutralized, but rather people who were struggling to live in the pressure cooker environment of what we call asymmetric warfare," PFC Manning added.

Journalists used these documents to uncover many startling truths. We learned...

- how Donald Rumsfeld and General Petraeus built their careers by supporting torture in Iraq.
- how deliberate civilian killings by U.S. forces in Iraq and Afghanistan went unpunished, and that thousands of civilian casualties were never acknowledged.
- most Guantanamo detainees were innocent.

For his service on behalf of an informed democracy, Bradley Manning faces life in prison. Prosecutors accuse him of "Aiding the Enemy" for providing WikiLeaks with this information, but acknowledged that they would have done the same if he had given the documents to *The New York Times*.

Nominated for the Nobel Peace Prize three years in a row, Bradley Manning is a whistle-blower in every sense of the term. He exposed secret crimes and malfeasance for the public good, and took nothing in return. Bradley Manning has accepted responsibility for releasing these documents and mishandling classified information. Alone, these charges could send him to prison for 20 years. Yet the Government argues for life in prison, declaring that he sought to indirectly aid our enemies with a new "open-source" espionage.

No proof that any lives were endangered, or that any person was even harmed, was presented by the prosecution.

A new whistle-blower, Edward Snowden, has stepped forward since Bradley Manning's trial began last month. He revealed that a vast, unwarranted, and fundamentally unconstitutional program of Internet and phone surveillance on every U.S. citizen is being conducted by the National Security Agency. Edward Snowden fled his home explaining that he feared the type of extreme punishment that Bradley Manning has already endured in military pre-trial confinement.

We put forward this letter to advance the public debate, as Bradley Manning intended—to further transparency and accountability in government. We dedicate ourselves to following Bradley Manning's example to expose the truth, even when inconvenient to do so. To promote openness in our government, so that it can be evaluated and improved. To believe, passionately, in the power of real democracy.

We await military judge Colonel Denise Lind's ruling as to what sentence Bradley Manning will receive in her Fort Meade, Maryland courtroom a few days from now. As PFC Manning has been imprisoned for over three years, and subjected to brutal conditions at Marine Base Quantico, Virginia for nine of those months, the only remotely reasonable sentence would be time-served.

We call on Major General Jeffrey Buchanan to use his ability as Convening Authority of these proceedings to reduce any sentence handed down by Judge Lind in order to free Bradley Manning without delay.

Finally, we call on President Barack Obama to pardon PFC Bradley Manning. This 25-year-old, openly gay soldier from Oklahoma does not deserve to spend one more day in prison for informing the public of our government's policies. Bradley Manning believed you, Mr. President, when you came into office promising the most transparent administration in history, and that you would protect whistle-blowers. **Now would be a good time to start upholding that pledged transparency, beginning with PFC Manning.**

We will not relent until this American hero is free.

Help us continue to pay for 100% of Bradley Manning's legal fees, including appeals if needed—in addition to grassroots education efforts.

Tax-deductible donations to the Bradley Manning defense fund payable to: **Courage to Resist / AFGJ**

Mail to: **Bradley Manning Support Network**
c/o Courage to Resist
484 Lake Park Ave #41, Oakland CA 94610

Facebook & Twitter: **savebradley** Phone: **510-488-3559**

To learn more, follow daily developments in the case, and to contribute to the defense fund online, please visit:
www.bradleymanning.org

Fuente: *The New York Times*.

Al igual que sucedió en la década de 1990 con los hackers perseguidos y encarcelados, las condenas disuasorias han tenido un efecto paradójico en este caso. Manning, como Kevin Mitnick y otros hackers arrestados, también ha sido encumbrado como héroe, sólo que ahora el héroe ya no es doméstico, sino global, un símbolo de la libertad en el mundo, encumbrado por diferentes actvistas, colectivos, organizaciones e instituciones vinculadas a los derechos civiles y las libertades. Por sus acciones, el exanalista ha sido reconocido con numerosos premios y distinciones: Premio Sam Adams (2014), de Sam Adams Associates for Integrity in Intelligence; Premio de la Paz

Sean Macbride 2013, del International Peace Bureau; Premio In His Footsteps 2013, del Harvey Milk LGBT Democratic Club; tres nominaciones al Premio Nobel de la Paz (2012, 2013 y 2014); Persona del Año 2012, concedido por el periódico *The Guardian*; Premio de la Paz 2013, de la US Peace Memorial Foundation; Premio Peacemaker del Año 2013, de The Peace & Justice Center of Sonoma County; Premio Hero of Peace 2013, de Eisenhower Chapter of Veterans for Peace; Premio SF Trans March 2013, de San Francisco Trans March; el SF Pride Grand Marshal Runner-Up 2013, de SF LGBT Pride former Grand Marshals, o el Premio People's Choice Human Rights 2012, de Global Exchange.

El desarrollo del juicio a Manning coincidió con el escándalo de las filtraciones de otro analista de la Agencia de Seguridad Nacional estadounidense, Edward Snowden, cuyas revelaciones sobre las prácticas de espionaje de esta agencia han evidenciado la realidad *orwelliana* tejida por el Estado-nación y las corporaciones transnacionales que dominan las redes de comunicación. El de Snowden no es un caso vinculado directamente a WikiLeaks y ni siquiera se puede describir como un *hack*, a diferencia de lo que hace WikiLeaks, como explica Stallman:

> En WikiLeaks hai un aspecto de *hack*. En el acto de Snowden no veo tanto de *hack*, el suyo es un acto político para actuar contra una tiranía, pero no he visto en Snowden el gusto del *hack* que si he visto en WikiLeaks. Tengo la impresión de que Assange gusta también de este aspecto de la inteligencia juguetona haciendo lo que hace (Richard Stallman, en Quian, 2013c).

Pero aunque el caso Snowden no se pueda describir como un *hack*, sí es fruto de la experiencia WikiLeaks y del aprendizaje que periodistas de *The Guardian* y *The Washington Post* obtuvieron de las colaboraciones con la organización liderada por Julian Assange (Leigh, 2015). En junio de 2013, Snowden —a quien Stallman, como a Julian Assange, considera un héroe (Quian, 2013c)— hizo públicos, a través de estos dos periódicos, documentos clasificados como alto secreto sobre varios programas de la NSA (National Security Agency), incluyendo los programas de vigilancia masiva PRISM y XKeyscore. Desde entonces, el goteo de filtraciones no ha cesado.

A Snowden se le atribuye la sustracción de 1,7 millones de archivos secretos de inteligencia que comprometen el sistema de espionaje y de vigilancia masiva de Estados Unidos. Por ello, el exanalista de la NSA se encuentra en paradero desconocido, en

algún lugar de Rusia, donde se le concedió un asilo temporal. Como Manning y Assange, Snowden también ha sido acusado de espionaje. El primero ha sido condenado a treinta y cinco años de prisión; el segundo ha tenido que recluirse en la embajada de Ecuador en Londres desde el 19 de junio de 2012 y ha pedido asilo a este país para evitar su extradición a Estados Unidos[176]; el tercero lleva una vida de fugitivo, saltando de país en país, y ha conseguido un permiso de asilo temporal en Rusia mientras aguarda que se resuelva alguna sus peticiones de asilo político a veintiún países: Alemania, Austria, Bolivia, Brasil, China, Cuba, Ecuador, España, Finlandia, Francia, Holanda, India, Islandia, Italia, Irlanda, Nicaragua, Noruega, Polonia, Rusia, Suiza y Venezuela (WikiLeaks, 2013).

[176] No es objeto de esta tesis abordar el controvertido y mediático proceso legal abierto en Suecia contra Julian Assange, a quien la Justicia de este país reclamó en 2010 con una orden de arresto para ser interrogado por dos presuntos casos de acoso sexual y otro de coerción ilegal, relacionados con una mujer, y otro presunto caso de violación en Suecia relacionado con otra mujer, de los cuales tres han prescrito; el único que ha quedado vigente es el de violación en grado menor. Consideramos desde un principio que este asunto pertenece al análisis jurídico de más alto grado, pero también pensamos que, tenga el desenlace que tenga, este caso personal no se puede vincular al examen de WikiLeaks como fenómeno informacional extraordinario. Que Assange se libre o responda de ese cargo ni mejora ni desvirtúa WikiLeaks, ni intensifica ni palidece su atractivo como objeto de estudio. En todo caso, sí consideramos radicalmente importante, por su sustancialidad, incluir en este pie de página una referencia al dictamen del 5 de febrero de 2016 —hecho público durante la fase final de revisión de esta tesis— del Grupo de Trabajo sobre Detenciones Arbitrarias de la ONU, que declara "arbitraria" la privación de libertad aplicada a Julian Assange, por lo cual reclama a Reino Unido y Suecia el fin de las medidas de privación contra éste y que reconozcan y satisfagan el derecho del fundador de WikiLeaks a una indemnización, lo cual coloca a Assange en el papel de acosado político. Véase:
- *The Working Group on Arbitrary Detention Deems the deprivation of liberty of Mr. Julian Assange as arbitrary*. Disponible en: http://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17012.
- *Julian Assange arbitrarily detained by Sweden and the UK, UN expert panel finds*. Disponible en: http://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17013.
Consultados ambos documentos el 6 de febrero de 2016.

IV.7. LA CONSTRUCCIÓN COLABORATIVA DEL MITO

IV.7.1. Un personaje en construcción

Julian Assange es un ser en construcción, un personaje que es policonstruido. En él, su pasado no tiene un valor biográfico sólido, sino que se sesga, se criba, se tamiza y se reinterpreta para (re)construir una identidad líquida presente e improvisar la narrativa vital de un personaje ulterior, en construcción, sometido al devenir de los de los acontecimientos y de sus relatos y que, por tanto, nunca *es* propiamente, ya que siempre está *siendo*. La narrativa vital se asemeja a un *collage*, a una colección de accidentes, de cosas encontradas e improvisadas que configuran el *yo* maleable descrito en Sennett (2000). El Julian Assange en construcción se adapta también a la definición de camaleón social en Gergen (1992), adoptando una personalidad pastiche que toma diferentes fragmentos de identidad según convenga al hacedor del personaje.

Esa construcción colaborativa del personaje es la que eleva a Assange al estatus de mito contemporáneo. En la construcción de este mito participan numerosos autores. Su historia es la suma de múltiples relatos con distintos escenarios y voces, en múltiples medios, soportes y formatos, y con numerosas evocaciones mitológicas e históricas, incontables representaciones hipermodernas y constantes puntos de empalme entre ficción y realidad. Julian Assange es un ser paradigmático de la convergencia cultural. En su caso, como icono de una legión de ciberlibertarios, observamos también el fenómeno de las comunidades de fans en la sociedad red descrito por el profesor Henry Jenkins:

> Los efectos políticos de estas comunidades de fans no dimanan simplemente de la producción y circulación de nuevas ideas (la lectura crítica de textos favoritos), sino también deI acceso a nuevas estructuras sociales (inteligencia colectiva) y nuevos modelos de producción cultural (cultura participativa). (Jenkins, 2008: 245).

Estamos, por lo tanto, ante un proceso en el cual la inteligencia colectiva genera un saber compartido (Jenkins, 2008).

Vamos a aproximarnos en los siguientes apartados de esta tesis a algunas contribuciones sustanciales en la construcción del mito Assange como fenómeno de la cultura de la convergencia de los medios de comunicación.

IV.7.2. Paralelismos con Daniel Ellsberg

Interesantes y reveladoras resultan las similitudes establecidas entre las figuras de Julian Assange y Daniel Ellsberg, el hombre que filtró en 1971 los conocidos como *Los Papeles del Pentágono* sobre la guerra de Vietnam (Sánchez Hernández, 2011). En sus entrevistas, Julian Assange hace reiteradas alusiones a Ellsberg como amigo, protector, aval. Las comparaciones surgieron desde el mismo momento que se conoció la existencia de WikiLeaks y ya fueron plasmadas en el primer artículo periodístico publicado sobre esta organización, firmado por Daniel Friedman en *Federal Times*, el 4 de enero de 2007:

> Bajo una cita del famoso filtrador de *Los Papeles del Pentágono* Daniel Ellsberg, www.Wikileaks.org dice que busca aumentar la transparencia del gobierno en todo el mundo mediante el uso de «una versión incensurable de Wikipedia para la filtración masiva de documentos no rastreables y su análisis» (Friedman, 2007).

Daniel Ellsberg fue calificado en 1971 por el entonces consejero de Seguridad Nacional de Estados Unidos, Henry Kissinger, como "el hombre más peligroso de América". Pero el mito de Julian Assange sobrepasa al de Ellsberg y al de cualquier enemigo del Estado-nación. Porque Assange es el primer enemigo público número uno hiperespacial y global. *The Most Dangerous Man in the World*, titula la biografía sobre Assange el periodista australiano Andrew Fowler; *My Time with Julian Assange at the World's Most Dangerous Website*, titula también su libro el exmiembro de WikiLeaks Daniel Domscheit-Berg, uno de los *traidores* del *mesías* del ciberespacio (la figura del traidor que vende al líder y, por ende, al grupo al que dirige, es esencial para contribuir a la mitificación y apología del mesías, pues sin Judas no hay crucifixión, resurrección, mitificación y deificación del mesías).

Otro importante paralelismo entre Assange y Ellsberg: la Administración Nixon puso en marcha en 1971 una unidad que se conocería como Los Fontaneros, cuyo objetivo era tapar filtraciones e intentar manchar clandestinamente la imagen de Ellsberg ante la opinión pública (aquel equipo provocó un año más tarde el estallido del escándalo *Watergate*, con el que se ha comparado el *Cablegate*). Algo muy similar hizo el Gobierno Obama: formar un equipo en el Pentágono de ciento veinte personas dedicadas en exclusiva a evaluar y limitar el impacto de las filtraciones de WikiLeaks, y a desprestigiar y criminalizar a Assange y a su organización. Una de las tareas

específicas encomendadas a este grupo, denominado WikiLeaks Task Force[177] —creado para operar en red por todo el mundo, dirigido por el Centro de Contrainteligencia de la CIA—, ha sido analizar si la capacidad de la agencia de inteligencia para reclutar informantes podría haber sido dañada por la disminución de la confianza en la capacidad del Gobierno de Estados Unidos para guardar sus secretos, a raíz de las filtraciones de WikiLeaks (Miller, 2010; Assange *et al.*, 2012: 15).

IV.7.3. Estrategia de personalización y personificación de los *mass media*

En el campo de los *mass media*, un buen ejemplo de estrategia de *storytelling* y contribución a la construcción del mito fue el encuentro que organizó el 3 de febrero de 2011 en Nueva York el Tow Center For Digital Journalism de la Columbia Journalism School, en el que lo más granado de la comunidad periodística anglosajona fue invitado a participar en la conferencia *WikiLeaks: The Inside Story*. El encuentro fue protagonizado por los dos grandes hacedores de esta historia: Bill Keller, editor en aquel momento de *The New York Times*, y Alan Rusbridger, editor también por entonces de *The Guardian*. Era el momento oportuno, nada casual, para presentar en sociedad, conjuntamente, los grandes relatos que sobre WikiLeaks y Julian Assange habían diseñado en sus despachos ambos editores y habían ordenado escribir a sus equipos. Assange acababa de romper relaciones con ambos periódicos y su hostilidad hacia éstos era manifiesta. *The New York Times* acababa de publicar el libro electrónico *Open Secrets. WikiLeaks, War and American Diplomacy*. Y *The Guardian* también había publicado otro libro, en papel: *Wikileaks. Inside Julian Assange's War on Secrecy*. La presentación de estos dos libros supuso el inicio del fin de la relación de Julian Assange con estos periódicos.

Sintomática es la descripción que *The New York Times* hace de su libro en el sitio web que creó *ex profeso* para promocionar el libro:

> *Open Secrets* es la crónica definitiva de la liberación de los documentos de WikiLeaks y la controversia que siguió. […] Tanto como un *thriller* legal y tecnológico, como también como manual para la política mundial, *Open Secrets* debe ser de especial interés para cualquiera que esté interesado en una de las historias periodísticas más persuasivas de nuestros días (www.nytimes.com/opensecrets).

[177] Según *The Washington Post*, en la CIA se le ha conocido principalmente por sus siglas en inglés, WTF, acrónimo popularmente utilizado en Intenet para expresar "What the fuck!" como expresión de asombro, estupefacción o desacuerdo.

En su libro, *The New York Times* reconstruye la historia de su *idilio* con Assange y ofrece una nueva versión, la del agraviado que desmitifica al amado, al que ahora dibuja como un tipo "inteligente y educado, extremadamente hábil con la tecnología, aunque arrogante, susceptible, conspirativo y extrañamente crédulo", y al que se somete a un juicio estético, describiéndolo como una persona desaliñada que viste ropa sucia y deteriorada y que "huele como si no se hubiese bañado en días" (Keller, 2011; Star, 2011: 18)[178]; una imagen opuesta a la que ofrece Assange en sus comparecencias públicas ante la prensa, cargadas de sofisticación.

Nada ha cambiado en tres décadas en los medios de masas. Es la misma trivialidad de la clásica retórica antihacker basada en convencionalismos estéticos y culturales, utilizada para describir y desprestigiar a estos apasionados de la computación, presentándolos como seres asociales que normalmente prestan poca atención a su apariencia física y cuidado corporal mientras son absorbidos por la tecnología en su actividad (Hafner y Lyon, 1996; Freedman y Mann 1997).

En su entrevista con el periodista Michael Hastings, de la revista *Rolling Stone*, Julian Assange interpreta este ataque personal como un arrebato de orgullo del editor Bill Keller y una muestra clara de su adhesión a los intereses del Gobierno estadounidense:

> Keller estaba intentando salvar su propio pellejo de la investigación de espionaje de dos maneras. La primera, mediante un tecnicismo legal, afirmando que no había habido colaboración, sino una relación pasiva entre periodista y fuente. La segunda, distanciándose de nosotros con el ataque personal, al más puro estilo amarillista de difamación. Muchos periodistas del *Times* me escribieron para decirme lo avergonzados que se sentían por ello. Keller también salió para decir lo contentos que estaban en la Casa Blanca porque el *Times* no había publicado el material de WikiLeaks que la Casa Blanca les había pedido que no publicaran. Una cosa es hacerlo, y otra es proclamarlo con orgullo. ¿Por qué sintió Keller la necesidad de decirle al mundo lo contestos que estaban en la Casa Blanca con ellos? Por la misma razón que sintió la necesidad de describir lo sucios que estaban mis calcetines. No para expresar algo concreto; más bien, para transmitir un alineamiento político (Assange, en Hastings, 2012: 48).

Julian Assange interpreta que los dos cabecillas de la gran alianza mediática que se había formado alrededor de WikiLeaks —*The Guardian* y *The New York Times*—

[178] Traducción propia.

habían iniciado una burda estrategia para desacreditarle, al recurrir a cuestiones banales —estéticas y personales— que desviaban la atención de lo verdaderamente importante. Para Assange, *The Guardian* y *The New York Times* estaban eludiendo sus responsabilidades:

> […] cuando *The Guardian* incumplió su contrato sobre el *Cablegate*, cuando le dijimos a *The New York Times* que no queríamos saber nada de ellos por su colaboración con la Casa Blanca, ambos grupos intentaron argumentar que lo complicado de mi carácter fue la razón por la que rompimos las relaciones. Dijimos que *The Guardian* incumplió su contrato, que el *Times* se dedicó al periodismo más zafio, sensacionalista y cobarde, así que la forma que encontraron de defenderse contra nuestros ataques fue decir: «Todo ha pasado porque los calcetines del señor Assange estaban sucios», o: «Es un tipo con el que trabajar resulta extremadamente difícil». (Assange, en Hastings, 2012: 50)

En la reconstrucción del personaje participó igualmente *The Guardian* con su también oportunista libro, en cuyo texto promocional se describe al fundador de WikiLeaks como "uno de los personajes más extraños en convertirse en una celebridad mundial"[179]. Uno de los párrafos más interesantes del libro para entender cómo los medios han contribuido a mitificar a Assange es éste, en el que se describe llegada del fundador de WikiLeaks a la Corte Suprema de Londres:

> Si los alienígenas hubieran aterrizado allí con su nave espacial, quizá habrían supuesto que uno de los santos de Dios estaba a punto de ascender al cielo. Julian Assange se había convertido, a ojos de muchos, en el san Sebastián de la era de Internet, un mártir atravesado por las muchas flechas de los no creyentes. Una *melée* de cámaras se apiñaba junto a la verja del tribunal de la ciudad de Westminster (Leigh y Harding, 2011: 251).

El afán de los medios por centrar la atención en el personaje y dejar en segundo plano el contenido de las filtraciones y, sobre todo, el mensaje de WikiLeaks (el medio es el mensaje, en sentido *mcluhaniano*), se pone de relieve en la investigación *Getting Personal: Personification vs. Data-Journalism as an International Trend in Reporting about Wikileaks*, en la que se hizo un análisis de contenido de los principales medios de comunicación de cinco países: España, Francia, Alemania, Suecia y Reino Unido. Dirigido por la profesora Andrea Czepeck (2011), en este estudio se analizan 1.125 noticias sobre WikiLeaks publicadas en diciembre de 2010, en el apogeo del *Cablegate*.

[179] Cita tomada de la página web promocional del libro de *The Guardian*: https://bookshop.theguardian.com/catalog/product/view/id/102211 (última consulta: 10 de enero de 2012).

La investigación concluye que hubo una clara tendencia a la homogeneización de la información y que la mayor parte de lo publicado fue superficial, sensacionalista y personalizado en Assange, en lugar de favorecer el esperado trabajo de investigación y análisis periodístico sobre los hechos y datos (Czepek, 2011: 94-95, 97).

Los investigadores descubrieron que sólo el 29,6 por ciento de las noticias se basaron directamente en los documentos filtrados por WikiLeaks. Y de éstas, casi la mitad —el 46,8 por ciento— aparecieron en *The Guardian*, el periódico que más artículos publicó sobre los documentos originales. Como revelador se presenta el siguiente dato: en el 51,9 por ciento de las piezas informativas analizadas no se mencionaron para nada los documentos; éstas se centraron en la historia y naturaleza de la organización WikiLeaks y en la causa penal contra Assange (Czepek, 2011: 100).

La personalización de la noticia fue notable en los medios estudiados. Así, un 31 por ciento de las piezas informativas se centraron en la figura de Assange y sólo un 8 por ciento mencionaron a otros miembros y partidarios de WikiLeaks. "Assange se convirtió en el rostro de WikiLeaks, sobre todo en televisión" (Czepek, 2011: 103).

Tabla 3: Menciones a Julian Assange en medios europeos.

Of items in...	mention Assange	Of items in...	mention Assange
France public tv	80%	France newspapers	37.5%
Germany public tv	59.4%	Germany newspapers	33.3%
Spain public tv	50%	Spain newspapers	30.9%
Sweden public tv	32.6%	Sweden newspapers	32.6%
UK public tv	31.3%	UK newspapers	26.5%

(Multiple actors were coded per item.)

Fuente: Diversity of Journalisms. Proceedings of ECREA/CICOM Conference, Pamplona, 4-5 de julio de 2011.

Este estudio refuerza las tesis que mantienen que, "en una espiral de referencias sinecdocales, WikiLeaks se convirtió en Assange y Assange se convirtió en la historia" (Uricchio, 2014: 2567). Por supuesto, en esta estrategia de personalización y personificación también tuvo mucho que ver la actitud del propio Julian Assange. Así lo

explican en su sexta tesis Lovink y Riemens (2010), que describen WikiLeaks como la típica SPO (*Single Person Organization*):

> Esto significa que la toma de iniciativas, de decisiones y la ejecución de las acciones se concentra en gran medida en las manos de una sola persona. […] Las SPO son muy reconocibles, emocionantes, inspiradoras y fáciles de cubrir por los media. La sostenibilidad de una SPO depende en gran medida de las actuaciones de su líder carismático, pero su funcionamiento no se concilia bien con los valores democráticos. Por eso mismo no admiten la puesta en cuestión ni la toma de decisiones en colectivo. El hacker soberano Julian Assange es la cabeza identificable de WikiLeaks, y la notoriedad y la reputación de Assange se funde con la de la organización misma. Lo que WikiLeaks hace o lo que apoya, se confunde con la propia agitada vida privada —en apariencia— de Assange y también con sus poco aseadas opiniones políticas (Lovink y Riemens, 2010: 142-143).

En el documental *WikiLeaks: Secrets and Lies* (2012), el periodista de *The Guardian* David Leigh recuerda el momento en que conoció personalmente a Julian Assange. Ese día, Leigh entendió inmediatamente que Assange era WikiLeaks. Fue el 23 de marzo de 2010, en Tønsberg, Noruega, en el encuentro anual de SKUP (Stiftelsen for en Kritisk og Undersøkende Presse), fundación para la investigación periodística. Así lo recuerda Leigh:

> Yo tenía que hablar en una conferencia periodística en Noruega y otro de los conferenciantes era Julian Assange. Esa fue la primera vez que comprendí que Julian era el centro de WikiLeaks, que él era WikiLeaks. La verdad es que los dos nos sentimos interesados, me senté a su lado en la cena. La verdad es que tiene una personalidad muy atractiva; es carismático (Leigh, en Forbes, 2011).

Aquella noche, Assange mostró a Leigh en privado el vídeo del asesinato de doce personas en Irak –entre ellas, dos empleados de Reuters– acribilladas por soldados estadounidenses desde un helicóptero. Pocos días después, el vídeo salió a la luz pública con el título *Collateral Murder*. Fue el primer gran golpe de efecto de WikiLeaks.

Durante el mes de diciembre de 2010, la atención de los medios sobre asuntos relacionados con WikiLeaks fue cayendo progresivamente en los cinco países analizados. Más de la mitad de todas las informaciones fueron publicadas la primera semana de diciembre, hasta el arresto de Assange el día 7. Hubo un pequeño repunte a mediados de diciembre, cuando Assange fue liberado bajo fianza, después de que en la mayoría de los medios de información WikiLeaks casi había desaparecido o había sido relegado a un segundo plano. Esto ocurrió a pesar de que en *The Guardian* y en el sitio

web de WikiLeaks se seguían revelando nuevos documentos, varios de ellos de más relevancia que los publicados a principios de diciembre (Czepek, 2011: 105). De esta forma, los medios fueron desviando la atención del público de los contenidos de las filtraciones y centrándola en la personalidad y la vida de Assange.

El estudio dirigido por la profesora Czepek también revela cómo los medios de comunicación contribuyeron a una dramatización de los eventos a través del lenguaje que utilizaron. Assange fue mitificado como "estrella de rock", "ángel exterminador" (*Der Spiegel*, 15 de diciembre), "genio hacker", "mártir de la libertad de expresión" (*Times*, 21 de diciembre), "nuevo vikingo", "luchador por la libertad" (*FAZ*, 17 de diciembre); o demonizado como "enemigo común" (*The Guardian*, 9 de diciembre) y "ciberterrorista" (*Times*, 21 de diciembre). Cuando grupos de hackers intentaron vengar a su líder por el bloqueo de grandes empresas a WikiLeaks, la acción fue dramatizada por los medios como "ciberguerra". "La dramatización se produjo en todos los medios de comunicación. Los medios que oficialmente o de otra manera colaboraron con WikiLeaks dramatizaron los acontecimientos, exagerando sus relevancia" (Czepek, 2011: 105). Esa dramatización era la mejor forma para los medios de comunicación de publicitar sus estrategias y hallazgos en el caso WikiLeaks.

Appelbaum considera que el control de la tecnología por quienes no comprenden su esencia explica el bombo que se ha dado a la ciberguerra en los últimos años:

> Básicamente se debe a que una serie de personas que parecen tener autoridad sobre la guerra empiezan a hablar sobre tecnología como si la entendieran. Estas personas hablan a menudo de la guerra, pero ninguna de ellas, ni siquiera una, habla sobre la ciberconstrucción de la paz, o de nada relacionado con la construcción de la paz. Hablan siempre de la guerra porque es su negocio, e intentan controlar los procesos tecnológicos y legales como medios para promover sus propios intereses (Assange *et al.*, 2012: 31-32).

De la investigación dirigida por Czepek se deduce, además, que los medios de comunicación, contra la idea extendida de que quisieron jugar un papel clave en la investigación periodística y en el apuntalamiento de un nuevo periodismo de datos y científico —descrito por López García, Toural Bran y Rodríguez Vázquez (2016) —, lo que hicieron realmente fue ejercer de *storytellers* para contar la historia de Julian Assange, aunque "resulta sorprendente comprobar que muchos medios de comunicación

no han hurgado más allá de tres *intros* para elaborar sus piezas sobre el creador de Wikileaks" (Plaza, 2011: 41).

Algunos de los clásicos males del periodismo moderno, descritos por el reportero y profesor Jim Nieken en su artículo 'Hack the Media' —publicado en la edición de invierno 1999-2000 de la revista *2600* (Goldstein, 2009: 261-265)—, parecen revitalizarse y diluir cualquier atisvo de regereneración: los plazos y la premura que dictan el trabajo del periodista coartan su capacidad de investigación, el tiempo reducido obstaculiza el análisis, y el rigor y la calidad de la información se sacrifican por la entrega rápida y masiva de un producto unitario, donde cada información sólo es una pieza más que debe encajar en una unidad total para su venta programada en el mercado de los medios de masas, que tienden a la simplificación, a una información básica y general para las masas estúpidas. Las empresas editoras de medios de información convencionales, no lo olvidemos, tienen un último y prioritario fin, que es ganar dinero, y la manera de ser rentables es ofreciendo historias que despierten el interés de las masas, exagerando, inclinando la historia, decorándola con artificios.

Julian Assange también ha lamentado el escaso interés que han mostrado los medios de comunicación, y en particular *The New York Times*, por los cables diplomáticos filtrados. El *Cablegate* consta de tres mil volúmenes de material y es, según Assange, el mayor tesoro intelectual que nunca se ha hecho público en tiempos modernos. Por eso lamenta que el *Times* publicara solamente unos cien cables de los 251.287 filtrados.

Sin embargo, y como ya hemos mencionado, sí hubo un urgente interés en acelerar la maquinaria del *storytelling* para relatar las experiencias de los periodistas con WikiLeaks, muy pronto transcritas en dos libros publicados a principios del año 2011 por *The New York Times* y *The Guardian*, centrados en la intrincada vida y personalidad de Julian Assange, en su ética y estética, y en su relación con los medios. La información y los datos de las filtraciones quedaron relegados por un relato ideado como obra dramática. Asi queda patente en el inicio del libro de *The Guardian*, en el que se nos presenta el elenco de actores de esta historia, antes de sumergirnos en ella[180].

[180] El libro de *The Guardian* sobre WikiLeaks comienza con el "Reparto", en la edición española, o "Cast of Characters", en la inglesa, donde se nos presentan los personajes de la historia, con sus nombres y sus respectivos papeles. En la versión española —editada por Deusto—, el "Reparto" se encuentra en las páginas 9-14.

Mención especial merecen las descripciones que sobre Assange aporta Bill Keller, con las que el exeditor de *The New York Times* hace aún más evidente la intención de los periodistas de novelizar sus encuentros (y desencuentros) con un personaje dual en el que conviven el héroe y el villano hacker:

> La fama de fugitivo transformó a Assange. El hombre desaliñado con mochila y calcetines caídos ahora llevaba el pelo teñido y arreglado, y prefería vestir a la moda con trajes ceñidos y corbatas. Se convirtió en una especie de figura de culto para los jóvenes e izquierdistas europeos, y era evidentemente un imán para las mujeres.
>
> […] Llegué a pensar en Julian Assange como un personaje de un *thriller* de Stieg Larsson, un hombre que podía entenderse como héroe o como villano en una de las novelas megaventas suecas que mezclan la contracultura hacker, la conspiración de alto nivel y el sexo como recreo y como violación (Keller, 2011; Star, 2011: 30-31)[181].

The New York Times y *The Guardian* han sido determinantes en el juicio, más que paralelo, en red, al que ha sido sometido el editor de WikiLeaks en la esfera pública:

> […] el furor de los medios sobre su vida personal le han convertido en un paria para la mayoría de los que simpatizaban con él, haciendo casi imposible la financiación. Se le ha llamado violador, combatiente enemigo y agente del Mossad y la CIA al mismo tiempo. Los que fueron sus dos principales colaboradores —los periódicos *The New York Times* y *The Guardian*— le han llamado repetidamente pervertido sexual con mala higiene personal mientras siguen vendiendo libros y derechos para el cine sobre sus hazañas tranquilamente. Su propia personalidad ha fomentado divisiones: es encantador, brillante e inflexible, pero ha inspirado un intenso odio por parte de sus antiguos colaboradores, que le acusan de ser un megalómano cuyo ego ha desprestigiado su causa (Hastings, 2012: 46).

En España, el diario *El País* también contribuyó de manera manifiesta a novelizar y mitificar la figura de Assange, y a personalizar y personificar el fenómeno WikiLeaks. En 'Cita secreta con el hombre que hace temblar al Pentágono', publicado un mes antes del *Cablegate*, el 24 de octubre de 2010, Joseba Elola preparó ya el terreno y nos introdujo en esta historia mitificando, por reiteración, la figura de Assange, deidad creadora de un universo lleno de galaxias de misterios y secretos. Obsérvese cómo *secreto* es la palabra clave del titular y del primer párrafo de la entrevista, donde Elola insiste hasta en cinco ocasiones en el secretismo que rodea a Assange y a WikiLeaks:

> Julian Assange vive en un universo de secretos. Secretos eran los 400.000 documentos sobre la guerra de Irak que liberó ayer. Secretos son los 30 envíos que cada

[181] Traducción propia.

> día recibe el portal que dirige, inagotable fuente de denuncia a escala planetaria. Secretas procuran ser sus comunicaciones, sus entradas y salidas. Su organización también vive envuelta en el más absoluto de los secretos (Elola, 2010).

"Secreta por tanto tenía que ser la cita con el hombre que se ha convertido en serio enemigo del todopoderoso Pentágono.", concluye y justifica el periodista de *El País*.

Elola construye en esta entrevista —la última concedida por Assange antes de su detención— un relato épico sobre "el último héroe del periodismo combativo", al que describe minuciosamente en la intimidad del cuerpo a cuerpo en un encuentro confidencial:

> Assange sabe cultivar los silencios. Habla mirando al horizonte, sus ojos se mueven de izquierda a derecha y de derecha a izquierda mientras busca la palabra precisa. Su voz grave, levemente quebrada, y su querencia por el susurro, más propio de la confidencia que de la entrevista, confiere aún mayor intensidad a sus palabras. Habla tan bajo que conduce al interlocutor a un compromiso de escucha insoslayable. O aguzas el oído, o no te enteras (Elola, 2010).

El periodista desarrolla el personaje novelizando el relato del drama familiar y las hazañas del joven hacker australiano:

> La existencia un tanto nómada no es algo que le resulte ajeno. «Nuestra familia producía teatro profesional y televisión y como resultado, íbamos de gira por el país muy a menudo», recuerda. Assange nació en 1971 en Townsville, ciudad de la costa noroeste australiana. Cuando tenía ocho años, sus padres se separaron. La madre inició una relación con un músico con el que tuvo otro hijo. «Durante una parte de mi adolescencia tuve que lidiar con este hombre del que se sospechaba estaba conectado con el culto de Anne Hamilton-Byrne», cuenta. Una secta en la que algunos miembros convencían a las madres para que ofrecieran a sus hijos recién nacidos a la líder del movimiento. Niños que se convertían en hijos adoptivos de la suma sacerdotisa, que ordenaba teñirles a todos el pelo de rubio y a los que se suministraban todo tipo de drogas, incluidas ceremonias de iniciación al LSD cuando apenas eran adolescentes.
>
> Llegó un momento en que no quedó otra salida que huir. Huir de las garras de aquel hombre. Assange, su hermanastro y su madre estuvieron tres meses cambiando constantemente de domicilio. Vivir a la fuga.
>
> Secretos y fugas. Dos conceptos que gobiernan la vida de Julian Assange. Leaks significa fuga. Y también fuga de información, filtración.
>
> Por aquellos años difíciles nació su fascinación por los ordenadores. Su pericia, sus dotes como programador, le convirtieron en un notable hacker. Su nombre de guerra: Mendax. Allí comenzó su lucha: la información está para ser compartida (Elola, 2010).

Lo contextualiza en el seno de una organización susceptible de traiciones y ataques despiadados:

> Cuenta que la organización ha recibido cien «ataques legales». Dos de cada cinco demandas/querellas acabaron en juicio. Asegura que salieron victoriosos en todos los casos. También destaca los ataques que le han dirigido los medios de comunicación. Se queja de que los medios replican las mentiras que otros deslizan y se retroalimentan ad infinítum manchando su biografía. «Ha habido 15 ataques contra nosotros completamente fabricados de arriba abajo», asevera, «vendidos como filtraciones de gente de dentro de la organización. Se ha llegado a decir que llevo una vida de lujo en Sudáfrica. Nunca he estado en Sudáfrica» (Elola, 2010).

Lo idealiza amplificando la voz del timonel de la verdad y gurú del cuarto poder; legitima su autoridad como prescriptor y futurólogo, y contrapone los dos grandes relatos sobre Assange:

> Para unos es el último héroe del periodismo, un hombre que desafía la lógica de un mundo cínico en busca de la máxima transparencia. Para otros, un idealista naif que cree que todo se puede contar, cuando hay cosas que el sentido común indica es mejor no publicar (Elola, 2010)..

Julian Assange puede ser, en definitiva, el héroe infalible o el idealista ingenuo, según quien narre el *cuento*, pero, en todo caso, personaje extraordinario, el ángel anunciador de "la muerte a escala mundial de la sociedad civil" (Elola, 2010) a manos de plutócratas.

Superado el estado de excitación periodística que causaron las filtraciones masivas de WikiLeaks durante el año 2010, el periodista David Leigh asumió en el documental *WikiLeaks: Secrets and Lies* que los periodistas de los medios que se habían coaligado para trabajar codo con codo con Assange habían convertido rápidamente a este hacker australiano y a su organización en "estrellas del rock" (Forbes, 2011). Assange y WikiLeaks debían su incipiente fama a los grandes medios tradicionales:

> Al publicarlo así, al exitir una colaboración entre tres grandes pubicaciones internacionales, todo el mundo prestó atención. Y en ese momento, WikiLeaks dejó de ser un grupo de chicos con una página web para ser una organización que podía cambiar el mundo (Leigh, en Forbes, 2011).

Assange es el Caballo de Troya del cuarto poder, convertido en pilar de las estructuras tradicionales del poder; o quizá es el líder de un movimiento neoanarquista que intenta destruir el Estado-nación desde su aparato de control y manipulación: los

mass media. La entrevista concedida a *El País* evidencia la utilización y manipulación que Assange ha hecho de los medios convencionales. Solemnizado, paradójicamente, por un medio de comunicación internacional tradicional, el fundador de WikiLeaks proclama:

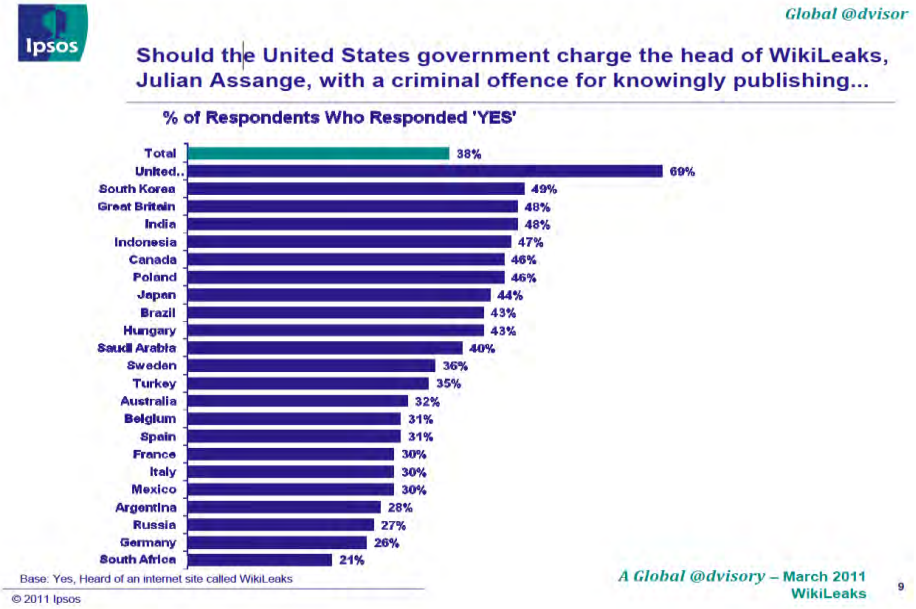
> Los medios de comunicación internacionales son un desastre. Estamos en una buena posición para verlo porque nos llega material política e históricamente significativo, lo liberamos, y vemos cuántos medios se hacen eco y con qué rigor. Podemos ver también los esfuerzos para suprimir la información que damos. Mi conclusión es que el entorno de los medios internacionales es tan malo y tan distorsionador que nos iría mejor si no hubiera ningún medio, ninguno (Elola, 2010).

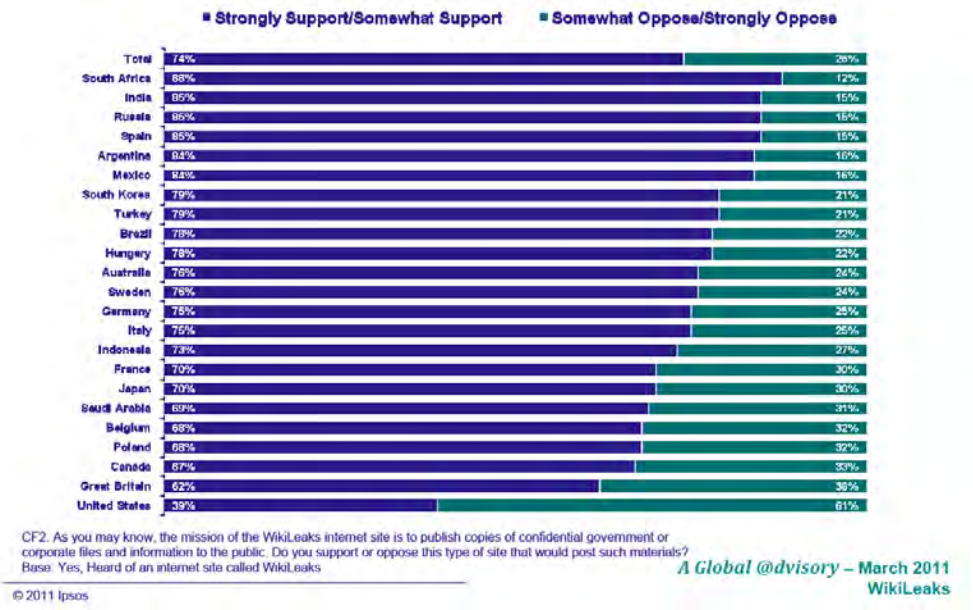
IV.7.4. Contrainformación: efectos en la opinión pública

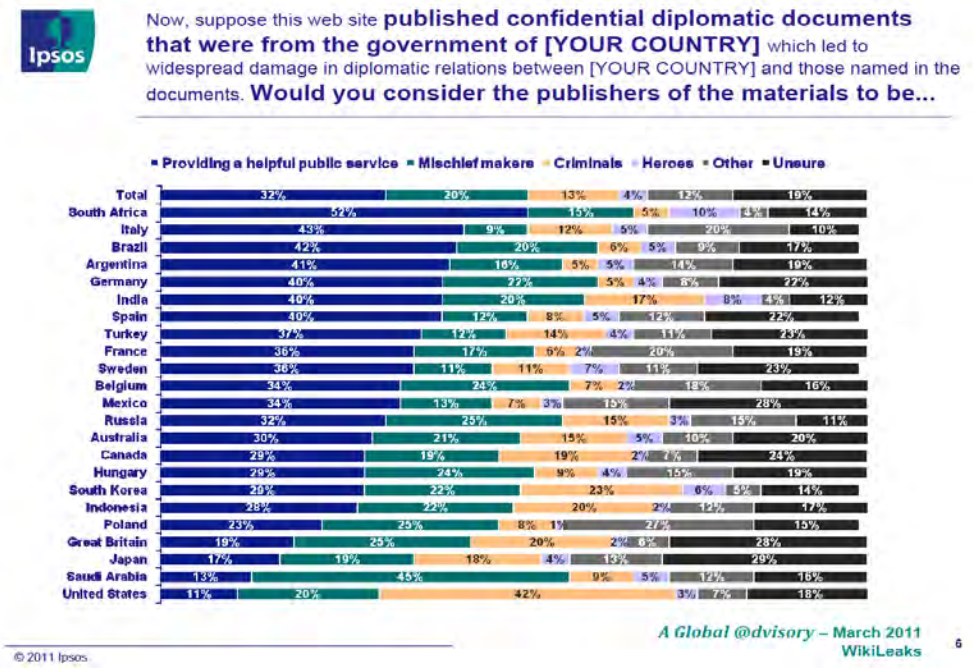
La labor de contrainformación del Gobierno de Estados Unidos tuvo efectos en la opinión pública de su país, como evidencia la encuesta internacional que Ipsos realizó entre el 2 y el 14 de marzo de 2011 a una población de 18.829 ciudadanos de veinticuatro países: Argentina, Australia, Bélgica, Brasil, Canadá, China, Francia, Gran Bretaña, Alemania, Hungría, India, Indonesia, Italia, Japón, México, Polonia, Rusia, Arabia Saudita, Sudáfrica, Corea del Sur, España, Suecia, Turquía y Estados Unidos.

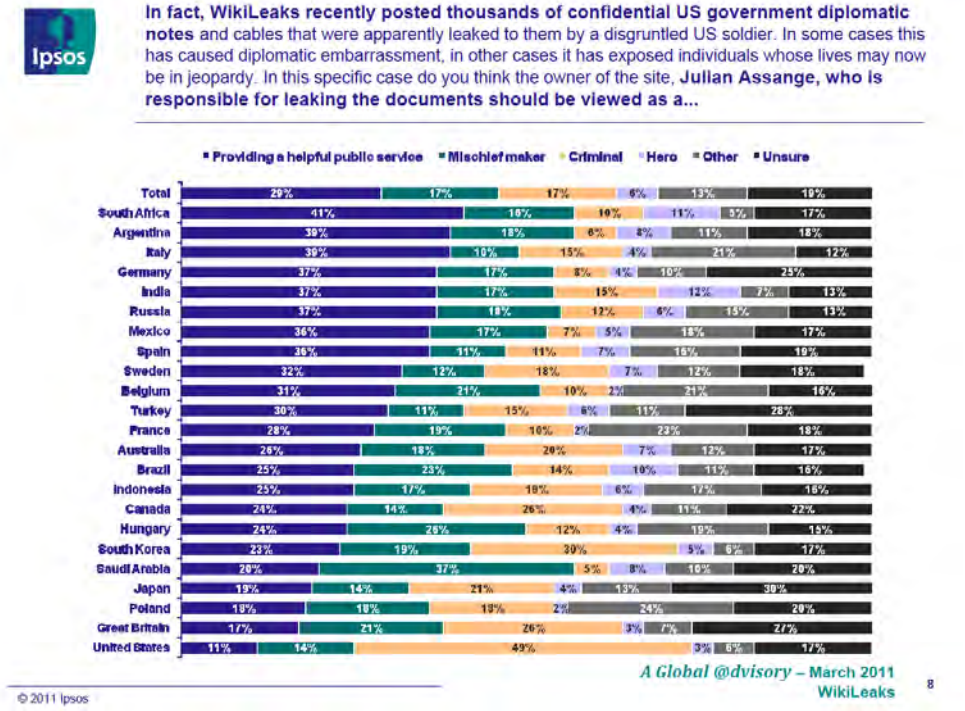
WikiLeaks ya era por entonces un fenómeno global. El 79 por ciento del total de los encuestados respondió haber oído hablar de un sitio en Internet llamado Wikileaks. Y el 74 por ciento dijo apoyar este tipo de sitios que publican documentos e información secreta de gobiernos y corporaciones. En todos los países, el porcentaje de aprobación superó el 60 por ciento, salvo en Estados Unidos, donde existía un rechazo mayoritario a este tipo de prácticas: apenas el 39 por ciento de los encuestados estadounidenses apoyó estas filtraciones y un 42 por ciento consideró que los editores de este tipo de materiales son unos "criminales", muy por encima de los porcentajes de otros países; el porcentaje en Estados Unidos se elevó hasta el 49 por ciento para calificar a Julian Assange como "criminal", otra vez muy por encima de los porcentajes en los demás países en los que se realizó la encuesta. De hecho, mientras en ningún otro país se alcanzó el 50 por ciento a favor de encausar a Julian Assange, el 69 por ciento de los estadounidenses opinó que su Gobierno debía procesar al fundador de Wikileaks (Ipsos, 2011).

Gráficos 7, 8, 9 y 10: Encuesta Ipsos sobre las filtraciones de WikiLeaks









Fuente: Ipsos.

WikiLeaks era percibida como una seria amenaza para los intereses de Estados Unidos. Su estrategia de impacto máximo estaba obteniendo resultados. A principios de abril 2010, cuando se publicó el vídeo del asesinato de doce personas desde un helicóptero Apache estadounidense en Irak, casi nadie había oído hablar de Assange. En

diciembre de ese año ya era uno de los personajes más famosos del planeta, con enemigos muy poderosos y amigos y admiradores muy apasionados (Manne, 2011).

IV.7.5. *Pop star*

Revistas tan prestigiosas como *Time*, *Forbes* y *Rolling Stone* también colaboraron de manera decisiva en la construcción del mito. En noviembre de 2010, *Forbes* colocó a Assange en el puesto 68 de las personas más poderosas del mundo. En diciembre también fue finalista en la lista de personajes del año de *Time* y el más votado por sus lectores. Ese mismo mes, la edición italiana de la *Rolling Stone* proclamó a Assange "rockstar de 2010". En la nota publicada el 13 de diciembre, la revista justifica así su decisión:

> Assange es icono como Che Guevara en las camisetas, como Mao para Andy Warhol. Es el jefe pop del fin de la diplomacia y de la seguridad imperial. Assange es la verdadera estrella del rock & roll de los Años Tresmil (Rolling Stone, 2010; Agencia EFE, 2010).

Assange también fue elegido persona más destacada de 2010 por la comunidad de la revista semanal estadounidense *The Nation* y por la redacción del diario francés *Le Monde*. Asimismo, en el informe *Twitter 2010: Year in review*, el *Cablegate* ocupó el séptimo puesto en el *ránking* de noticias más divulgadas en esta red social y Assange fue el cuarto personaje más popular, sólo superado por Justin Bieber, Dilma Rouseff y Lady Gaga, en este orden.

Cuadro 10: Ránking de temas y personajes más populares en Twitter en 2010.

NEWS EVENTS	PEOPLE
1. Gulf Oil Spill	1. Justin Bieber
2. Haiti Earthquake	2. Dilma Rouseff
3. Pakistan Floods	3. Lady Gaga
4. Koreas Conflict	4. Julian Assange
5. Chilean Miners Rescue	5. Mel Gibson
6. Chavez Tas Ponchao	6. Lil Kim
7. Wikileaks Cablegate	7. Zilda Arns
8. Hurricane Earl	8. Kate Middleton
9. Prince Williams Engagement	9. Kim Hee Chul
10. World Aids Day	10. Joannie Rochette

Fuente: *Twitter 2010. Year in review*.

Los distintos escenarios en los que se ha desarrollado la trama judicial han ayudado también a diluir las fronteras entre realidad y ficción y a reforzar el mito a través de paralelismos históricos, metáforas visuales y sugerencias y comparaciones novelescas y cinematográficas: el Londres de Guy Fawkes y *V de Vendetta*; las puertas neogóticas de la Corte Suprema londinense; la vetusta prisión de Wandsworth, del siglo XIX, que en 1895 alojó a otro mártir intelectual admirado por Assange, el escritor Oscar Wilde; o la Suecia del intrépido periodista Mikael Blomkvist y la hacker andrógina y neogótica Lisbeth Salander, personajes del *best-seller Millennium*, de Stieg Larsson.

Los premios también han contribuido a la mitificación. En 2008, Assange recibió el premio Index on Censorship de la revista británica *The Economist*; en 2009 fue premiado por Amnistía Internacional por unos documentos que revelaban ejecuciones sumarias en Kenya; en 2010 recibió el Premio Sam Adams, el Premio José Couso de Libertad de Prensa que conceden el Colexio Profesional de Xornalistas de Galicia y el Club de Prensa de Ferrol; en 2011, la medalla de oro de la Sydney Peace Foundation, el Walkley australiano y el Premio Internacional Libertad de Prensa, instituido por la Cátedra Unesco de la Universidad de Málaga, entre otros galardones. WikiLeaks incluso fue nominada en 2011 al Premio Nobel de la Paz por su contribución a la libertad de expresión y la transparencia, y por revelar corrupciones y violaciones del derecho internacional por parte de gobiernos y empresas.

IV.7.6. Prometeo *postcypherpunk*

En Julian Assange convergen arquetipos de la mitología clásica y de la cultura pop; el personaje histórico clásico y el postmoderno; lo real y lo fabulado; la ciencia y la ficción; el héroe y el villano; los medios tradicionales y los digitales alternativos; el entretenimiento y la información. Julian Assange es un Prometeo *postcyberpunk* en el hiperespacio.

Una de las comparaciones más recurrentes para describir a Assange es la que se establece con Neo, personaje protagonista de *The Matrix*, película del género *cyberpunk*: "Matrix toma prestados estos arquetipos tanto de los géneros de entretenimiento popular (el hacker protagonista, el movimiento de resistencia, los misteriosos hombres de negro) como de las fuentes mitológicas (Morfeo, Perséfone, El Oráculo)" (Jenkins, 2008: 126). En Julian Assange identificamos también a un hacker

líder de un movimiento de resistencia que ha evolucionado del *cypherpunk* y que bebe de la mitología griega. Pero no estamos ante un héroe de ficción o ante un titán mitológico, sino ante un héroe tangible, real, que invita a ficcionar su vida: como Prometeo, Assange desobedece las normas y roba el conocimiento (la verdad) de los dioses (Estado-nación, corporaciones) para dárselo al ser humano.

Prometeo es el titán rebelde, libertario, benefactor y amigo de los humanos, portador del fuego y de sucesivas tecnologías, que desafía a Zeus y el orden del Olimpo. Por su ofensa y osadía de otorgar a los mortales el poder divino, es castigado y encadenado a una roca (las cadenas de la censura).

Las comparaciones con Prometeo parecen inevitables en el caso de Assange:

> […] recientemente ha surgido un nuevo Prometeo que ha vuelto a robar el fuego del Olimpo. El héroe mitológico se ha encarnado en Julian Assange, el creador de Wikileaks, al que han encadenado para dejarlo a merced de las alimañas. Ha sido el primero, pero pronto tendrá una legión de seguidores dispuestos a apropiarse de la alta tecnología informática, como del fuego sagrado, y entonces serán los corderos los que desafíen y suplanten a los dioses (Vicent, 2011).

La metáfora de Prometeo ha sido manejada también por autores como Milan (2013) o Karatzogianni y Robinson (2014) para describir a aquellos grupos o individuos que, como el osado titán mitológico, están dispuestos a *robar* el *fuego.* Individuos, muchos de ellos, que se cultivaron en la lista de correo *Cypherpunks* y en los que se inspiraron otras nuevas generaciones de punks de la criptografía, como así reconoce Appelbaum:

> Al ver el trabajo de Julian [Assange] me di cuenta de que la tecnología se podía usar para conferir a la gente de a pie el poder de cambiar el mundo. Remontándome en el tiempo, a los tiempos de la vieja lista de correo *Cypherpunks* con Tim May, uno de los miembros fundadores del movimiento, y leyendo las antiguas entradas de Julian en esta lista, estoy convencido de que eso fue la génesis de toda una generación que pronto adoptaría posturas más radicales, porque la gente empezó a darse cuenta de que podía acabar con la atomización que padecía, que podía dedicar algo de tiempo a escribir un tipo de software que empoderara a millones de personas (Assange *et al.*, 2012: 70-71).

La investigadora Stefania Milan ofrece su particular visión en esta reinterpretación contemporánea de Prometeo:

> «Fuego» aquí es una metáfora de la tecnología y de la infraestructura de comunicación […]. Robar significa «reclamar y reapropiarse» estas infraestructuras de

> comunicación para establecer medios autónomos de comunicación […]. Al «robar el fuego», estos nuevos Prometeos intentan romper el monopolio de los Estados, así como el de los conglomerados mediáticos, informáticos y de telecomunicaciones […] sobre el uso y control de la infraestructura de comunicación. Su objetivo es permitir a otros grupos sociales transmitir su mensajes propios, sin pasar por los filtros de guardianes comerciales o estatales (Milan, 2013: 1)[182].

Como ya hemos visto, para comprender las motivaciones políticas de Assange debemos adentrarnos en el movimiento *cypherpunk* surgido en los años noventa del siglo XX, cuando hackers y ciberlibertarios expertos en criptografía tomaron el *cyberpunk* como fuente de inspiración. A la par, también en la década de 1990 surgió el *postcyberpunk*, otro subgénero de ciencia ficción que evolucionó del *cyberpunk*. Pero a diferencia de éste, donde sus personajes actúan como lobos solitarios y desconectados socialmente, los personajes *postcyberpunks* se muestran más involucrados en la sociedad en la que se desenvuelven y actúan para defender un orden social establecido o para crear una sociedad mejor (Person, 1998). Frente al enfatizado efecto alienante de las nuevas tecnologías en el *cyberpunk*, en el *postcyberpunk* la sociedad encuentra en en los artefactos tecnológicos una suerte de objeto mágico redentor o emancipador. Esa misma actitud hacia la tecnología y una motivación por cambiar el mundo son las que adopta Julian Assange. En la entrevista con Michael Hastings para la *Rolling Stone*, se reconoce como una persona formada en "experiencias relacionadas con la lucha por la libertad de prensa, la libertad para la comunicación del conocimiento, que, en último término, es la liberación de la ignorancia" (Assange, en Hastings, 2012: 48).

En Assange encontramos atributos propios de un personaje *postcyberpunk* que quiere superar percepciones distópicas para idear un mundo utópico. Assange está muy lejos de poder ser interpretado como un personaje *cyberpunk* marginal o un alienado solitario, pues se muestra como un líder protegido por numerosos amigos y grupos de apoyo, por anónimos y por destacados líderes de opinión, y es también un hombre con un relato de vida familiar, algo impropio del *cyberpunk*. Además, se ha socializado en la Red de redes y, lejos de recrearse en distopías y en el vacío deontológico, se dota de valores éticos y confía en la alta tecnología para el desarrollo de una sociedad transparente e idealizada, basada en la justicia social, que difiere radicalmente de los universos distópicos *cyberpunks* y del *darwinismo* tecnológico *cypherpunk*. La clave

[182] Traducción propia.

para alcanzar, ahora sí, la utopía, está en desmantelar la censura y el secreto como subterfugio de los Estados-nación y de corporaciones. Pero también pasa por dotar a todos los seres humanos de las habilidades para superar la distopía.

Si bien el movimiento *cypherpunk* coincide con el *postcyberpunk* no sólo en el tiempo —ambos surgen en la década de 1990—, sino también en la confianza en las nuevas tecnologías para la construcción de un futuro mejor, el *cypherpunk*, al menos en sus orígenes, marcados por la corriente anarcocapitalista liderada por Tim May, ha desechado conceptos como los de «justicia social», «solidaridad» o «bien común». Por todo esto, consideramos más preciso decir que Julian Assange es un *postcypherpunk* que ha superado la radicalidad extrema de los primeros *cypherpunks*, cuya corriente dominante no contemplaba convertirse en benefactora de la humanidad, sino en una elite meritocrática a salvo de la distopía en la que quedaría atrapada el resto de la humanidad, en un mundo sin límites morales.

El nuevo Prometeo es un libertario *postcypherpunk* que comparte los valores de la cultura hacker y, principalmente, la creencia de esta comunidad en la reinvención de la sociedad a través del progreso tecnológico abierto y libre. Y es por ello por lo que es castigado por los *dioses* del Olimpo (los Estados-nación), por usurpar su fuente de poder (la información) para entregársela al pueblo.

IV.7.7. Factoría transmediática

Julian Assange y WikiLeaks han generado a su alrededor una inmensa producción de obras narrativas en distintos medios, formatos, soportes y géneros, en las que realidad y ficción se entreveran dando lugar a diversos relatos sobre el personaje y su universo. La historia de Assange y el fenómeno WikiLeaks salpica a la política mundial, pero también a la industria de los medios, de la cultura y del ocio, algo a lo que ha contribuido también de manera decisiva el propio Assange, quien ha llegado incluso a confundir su identidad personal con una marca transnacional.

Por medio de sus abogados del bufete Finers Stephens Innocent, Assange presentó el 14 de febrero de 2011 ante la oficina de patentes de Reino Unido una petición para convertir su nombre en marca registrada y proteger así su uso para diversos servicios, como conferencias o servicios de noticias, entretenimiento o

educación. La marca 'Julian Assange' entró definitivamente en el registro de la Intellectual Property Office británica el 13 de marzo de 2011 y es renovable cada diez años.

Cuadro 11: Registro de la marca Julian Assange.

Intellectual Property Office

Case details for trade mark UK00002572177

New Search View historic case details Glossary of terms Print Friendly View

Trade mark

Trade mark:	JULIAN ASSANGE
Status:	Registered

Relevant dates

Filing date:	14 February 2011
Date of entry in register:	13 May 2011
Renewal date:	14 February 2021

List of services

Class 41:	Public speaking services; news reporter services; journalism; publication of texts other than publicity texts; education services; entertainment services.

Name and Address details

Owner(s) name:	Julian Assange c/o Finers Stephens Innocent LLP, 179 Great Portland Street, London, United Kingdom, W1W 5LS

View owner's other trade marks

IPO representative name:	Saunders & Dolleymore LLP 9 Rickmansworth Road, Watford, United Kingdom, WD18 0JU

Publication details

First advert:	Journal : 6877 Date of publication : 04 March 2011

Fuente: captura de pantalla propia tomada de https://www.ipo.gov.uk/tmcase/Results/1/UK00002572177.

Convertir a Assange en marca registrada contribuye a su cosificación en una campaña mundial de márketing y contradice, a todas luces, principios de la ética hacker contrarios a los derechos privativos y exclusivos de la propiedad intelectual. Los abogados de Assange alegaron que la intención es proteger el nombre de su representado para impedir que pudiese ser usado con fines lucrativos por terceros (Barkham, 2011).

Julian Assange y WikiLeaks se han convertido, como un *todo*, en un fenómeno paradigmático de la convergencia mediática, la cultura participativa y la inteligencia colectiva, conceptos emergentes para realidades emergentes definidos y entrelazados por Jenkins (2008) para describir un cambio de paradigma cultural que se ha producido

en nuestras mentes y en nuestra manera de interactuar con la realidad a través del uso de los medios de comunicación. A este cambio de paradigma Jenkins lo llama cultura de la convergencia, "donde chocan los viejos y los nuevos medios, donde los medios populares se entrecruzan con los corporativos, donde el poder del productor y del consumidor mediáticos interaccionan de maneras impredecibles" (2008: 14).

La cultura de la convergencia en Jenkins se refiere al flujo de contenidos a través de múltiples plataformas mediáticas, la cooperación entre múltiples industrias mediáticas y el comportamiento migratorio de las audiencias mediáticas, motivadas y dispuestas a ir casi a cualquier parte en busca de nueva información y del tipo deseado de experiencias de entretenimiento, y a establecer conexiones entre contenidos mediáticos dispersos. Esta circulación de contenidos mediáticos (a través de diferentes sistemas mediáticos, economías mediáticas en competencia y fronteras nacionales) depende enormemente de la participación activa de los consumidores, cuya proactividad ahora contribuye a configurar una cultura participativa que contrasta con nociones más antiguas del espectador pasivo. En lugar de hablar de productores y consumidores mediáticos como si desempeñasen roles separados, Jenkins recoge y redefine el concepto de prosumidor anticipado primero por McLuhan y Nevitt (1972) y luego formalizado por Toffler (1980), para definir las nuevas reglas de participación en la cultura emergente. Para Jenkins, la convergencia no tiene lugar mediante aparatos mediáticos, por sofisticados que éstos puedan llegar a ser, sino en el cerebro de las personas y mediante sus interacciones sociales con otros, de las que surge una inteligencia colectiva que es fuente alternativa de poder mediático y que contribuye a la creación colectiva de nuevos significados dentro de la cultura popular que afecta a los modos de operar de la religión, la educación, el derecho, la política, la publicidad e incluso el mundo militar (Jenkins, 2008: 14-15).

En este nuevo paradigma, WikiLeaks emerge como fenómeno transmediático e hiperespacial que se conoce y experimenta a partir de fragmentos de información que se propalan por el espacio cíber y el espacio físico, tocándolo casi todo: la política, los medios de comunicación, el periodismo, la industria del conocimiento, la cultura del ocio, la Academia, etc. Las filtraciones de documentos secretos a través de medios físicos y electrónicos son sólo una parte del universo WikiLeaks, que se expande también materializado, como ya hemos visto, en programas políticos y acciones de

protesta civil híbridas, pero también en libros, películas, videojuegos, programas de televisión, memes, *merchandising*, conferencias, etc.

Veamos ahora algunos ejemplos tempranos de convergencia mediática, cultura participativa e inteligencia colectiva alrededor de Julian Assange y WikiLeaks.

En las semanas siguientes a la publicación de los cables entre las embajadas estadounidenses y el Pentágono, el popular actor Bill Hader empezó a parodiar a Julian Assange en el célebre *late show* de la cadena NBC estadounidense *Saturday Night Live*.

> Este retrato cómico de Assange más o menos definía la forma en que estaba siendo percibido por el público: para algunos era un encanto engreído que podía hacer cualquier cosa en nombre de «la libertad de expresión»; para otros era un burro que no tenía respeto alguno por la ley, la seguridad del gobierno o la democracia (Solís, 2011).

Ilustración 37: Bill Hader, en el papel de Julian Assange en *Saturday Night Live*.

Fuente: captura de pantalla propia tomada de NBC.com

Hader originó el 18 de diciembre de 2010 uno de los memes más famosos sobre Julian Assange y WikiLeaks que han circulado por la Red. Después de que *Time* nombrara a Mark Zuckerberg Persona del Año 2010, a pesar de que Assange había sido el más votado por los lectores de la revista, Hader, en el papel de Assange, ironizó en televisión:

> ¿Cuáles son las diferencias entre Mark Zuckerberg y yo? Yo te doy información privada de las corporaciones, gratis, y soy el villano. Mark Zuckerberg le da tu información privada a las corporaciones a cambio de dinero y él es el «Hombre del Año» (Bill Hader, en *Saturday Night Live*, 2010).

Esta actuación de Hader se convirtió en un auténtico fenómeno en Internet y se viralizó hasta tal extremo, que en muchos sitios de la Red esas palabras se le han atribuido a Julian Assange y se han convertido en epígrafe de muchos relatos en la Red sobre el editor de WikiLeaks. Este meme contribuyó también a fortalecer el discurso de Assange contra Facebook y a fijar a Zuckerberg como su antagonista en la consciencia colectiva.

Ilustración 38: Meme de Julian Assange y Mark Zuckerberg.

Fuente: https://www.jitbit.com/alexblog/222-julian-assange-vs-mark-zuckerberg/.

Este meme constataba una realidad:

> Facebook tiene una reserva de información más íntima y más rica de sus ciudadanos que la que cualquier nación haya tenido nunca, y el Gobierno de Estados Unidos llama a veces a su puerta, citación en mano, para pedir prestada alguna de esa información (Grossman, 2010)[183].

Mientras que se puede decir que:

> WikiLeaks tiene la mayor reserva independiente de información sobre diversos gobiernos y empresas privadas, y en contraste con la espontánea y amable visita en Palo Alto [a Facebook], los federales están más interesados en derribar la puerta de WikiLeaks que en llamar a esta (Andrejevic 2014: 2620).

También en diciembre de 2010, el canal de humor *online* Small Poppy TV presentó en YouTube una pieza de dibujos animados en la que Oprah Winfrey, la popular estrella de la televisión en Estados Unidos, viaja a Australia para entrevistar a

[183] Traducción propia.

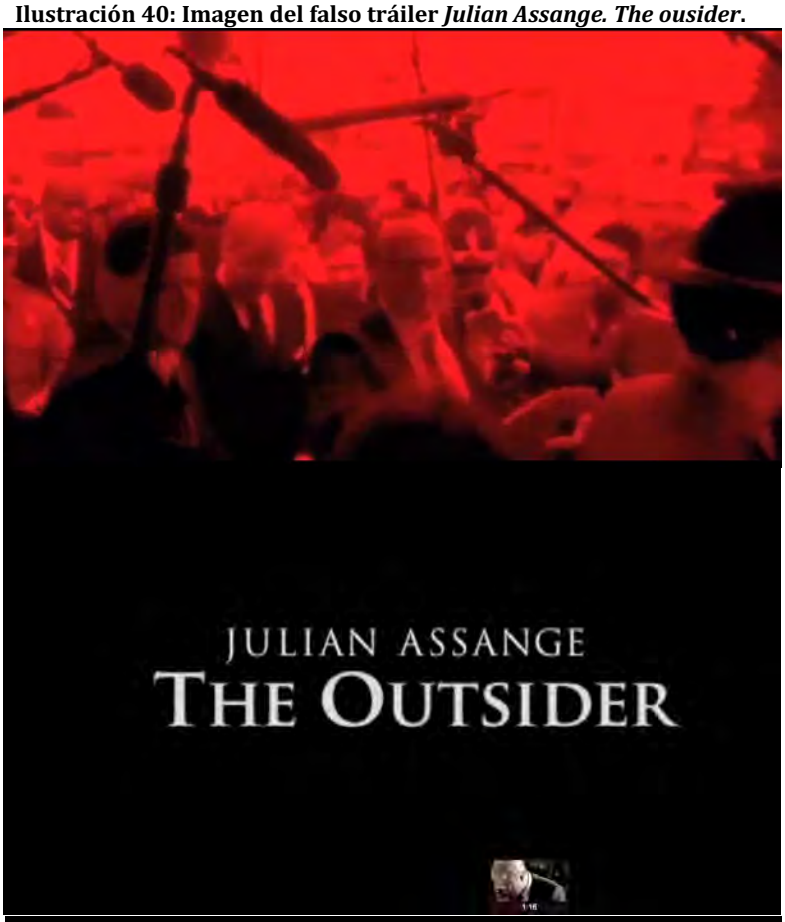
un Julian Assange que ha estado ocultándose junto con Bin Laden (líder del grupo terrorista Al Qaeda) y Wally (el escurridizo personaje de jersey de rayas rojas y blancas de la popular serie de libros de juegos *Where's Wally?*).

Ilustración 39: Escena de un capítulo de Small Poppy TV con Julian Assange, Bin Laden y Wally.

Fuente: captura de pantalla propia tomada de Small Poppy TV en http://youtu.be/TtsoxxCsY0I.

Entre la multitud de vídeos que encontramos en YouTube sobre Julian Assange destacamos también un *remake* del tráiler de la película *The Insider* (1999), dirigida por Michael Mann y protagonizada por Al Pacino en el papel del director del programa *60 Minutes* del canal CBS, quien destapa todos los trapos sucios de la industria del tabaco gracias a un confidente y antiguo bioquímico de la tabacalera Brown & Williamson, al que da vida el actor australiano Russell Crowe. En este *remake*, titulado *Julian Assange: The Outsider - The WikiLeaks movie trailer*, además de aprovecharse cierto parecido físico del confidente con Assange, el montaje favorece y enfatiza similitudes de la película con el caso del fundador de WikiLeaks a través de la selección de escenas y frases del filme que encajan perfectamente en la historia de Assange. Las escenas de ficción se combinan en este tráiler con cortes reales de los informativos de varias cadenas de televisión en los que se informa sobre las filtraciones de WikiLeaks, y con una voz en *off* que reescribe el guión de la película para presentarnos una fascinante historia "basada en hechos reales", la de Julian Assange, el *outsider*. Este vídeo fue publicado en YouTube el 16 de diciembre de 2010.

Ilustración 40: Imagen del falso tráiler *Julian Assange. The ousider*.



Fuente: captura de pantalla propia tomada de http://youtu.be/Qc08KyYYRgI

Un fenómeno a destacar es el de los juegos *online* sobre el caso WikiLeaks. Para aglutinar todos los juegos *online* que se iban creando sobre esta historia se publicó la página web colaborativa *Wikileaks Stories (wikileaks-stories.com)*[184], donde se animaba a crear y compartir juegos para "apoyar a WikiLeaks y difundir la información reveladora contenida en sus filtraciones a través del medio interactivo, y utilizar el poder de los juegos para luchar por la democracia y la libertad", según explicaban sus creadores en este sitio web. Algunos juegos compartidos fueron: *Leaky World*, una reinterpretación interactiva del ensayo de Julian Assange *Conspiracy as Governance*; *You Shall Know The Truth*, una sátira oscura en la que un agente secreto trabaja para recuperar información de WikiLeaks; *Wikileakers*, en el que la misión es liberar todos los cables diplomáticos y apoyar a Assange, que se encuentra bajo el *fuego* de Estados

184 Este sitio web fue desactivado, aunque aún se puede encontrar un registro de su actividad en su cuenta en Facebook, en la que su última publicación data del 22 de diciembre de 2012: https://www.facebook.com/Wikileaks-Stories-174777262542966/ (último acceso: 7 de abril de 2013).

Unidos y de sus aliados; *Uncle Sam vs WikiLeaks*, otra sátira sobre el poder estadounidense en la que el *Tío Sam* debe destruir a golpes los servidores de WikiLeaks; *WikiLeaks: The Game*, donde un pícaro y escurridizo Julian Assange se introduce en el Despacho Oval, donde debe conectar su *pendrive* al ordenador de Barack Obama para copiar sus archivos sin que éste se percate; *Cablegate: The Game*, un juego colaborativo que ofrece a los participantes los cables diplomáticos de las embajadas de Estados Unidos revelados por WikiLeaks para que los etiqueten y los resuman, y ayuden así a una mejor categorización y comprensión de los documentos filtrados.

Ilustración 41: Imagen del videojuego *WikiLeaks: The Game*.

Fuente: captura de pantalla propia tomada de http://www.jeuxjeuxjeux.fr/jeu/ne+te+fais+pas+attraper/wikile

Otro sitio web que recopiló nuevas narraciones sobre Assange y su organización fue *WikiLeaks Movie* (*wikileaks-movie.com*)[185]. Esta página web fue un gran repositorio de noticias y referencias sobre numerosos libros y proyectos audiovisuales para cine, televisión e Internet centrados en Assange y WikiLeaks. Se ideó como un proyecto colaborativo independiente auspiciado por Imagine Publishing, Inc. y desarrollado por voluntarios. Aquí encontramos información sobre los proyectos de cineastas consagrados y grandes estudios, pero también sobre los trabajos de creadores independientes y *art projects* de ciudadanos de todo el mundo.

185 Este sitio web también fue desactivado. En su cuenta en Twitter, su última publicación data del 23 de octubre de 2011: https://twitter.com/iwikileaksmovie (último acceso: 7 de abril de 2013).

Ilustración 42: The Wikileaks-Movie.com Project

Fuente: http://www.crowdsourcing.org/site/wikileaks---movie-/wikileaks-moviecom/6255

La producción literaria comercial sobre Julian Assange y WikiLeaks también empezó a ser vasta tras las masivas filtraciones del año 2010. En la lista de los numerosos libros que fueron apareciendo sobre Assange y su organización destacan, como primeras ofertas a los lectores: *Inside Julian Assange's War on Secrecy*, escrito por los periodistas de *The Guardian* David Leigh y Luke Harding; *Open secrets: WikiLeaks, War and American Diplomacy*, libro coral editado por *The New York Times* con aportaciones de reporteros, de analistas y del exeditor Bill Keller; *Julian Assange: The Unauthorised Autobiography*, una polémica autobiografía editada por Canongate Books y escrita, tras horas de entrevistas con Assange, por Andrew O'Hagan, quien decidió no firmar la obra tras romperse el acuerdo al que se había llegado con el fundador de WikiLeaks por el que éste revisaría el contenido antes de su publicación; *Desmontando WikiLeaks*, una controvertida mirada del escritor superventas Daniel

Estulin, exagente de contraespionaje de la KGB, en la que alimenta las teorías de la conspiración contra WikiLeaks; *The Most Dangerous Man in the World*, biografía sobre Assange del periodista australiano Andrew Fowler; *My Time with Julian Assange at the World's Most Dangerous Website*, de Daniel Domscheit-Berg, excolaborador de Assange y fundador de OpenLeaks (clon de WikiLeaks), considerado por Assange y sus seguidores un traidor resentido; o en España, *W de WikiLeaks. La venganza contra las mentiras del poder*, de Bruno Cardeñosa, director de la revista española *Historia de Iberia Vieja* y presentador del programa radiofónico *La Rosa de los Vientos*.

Especial atención requiere la producción literaria desarrollada por el propio Julian Assange, quien encontró en la literatura comercial otra vía para seguir agitando conciencias y narrar su propia versión, aprovechando su fama ganada como nuevo icono de la cultura popular y el tirón comercial de su figura y de WikiLeaks. Un claro ejemplo de ello son sus libros *Cypherpunks* y *When Google Met WikiLeaks*.

Consciente del poder de difusión e impacto intelectual que aún tiene la vieja industria capitalista del conocimiento, Assange se ha valido de ésta en su estrategia de expandir el universo WikiLeaks por todas las vías posibles, incluyendo la vieja prensa y la televisión, pero también la industria del libro. Las urgencias de los tiempos virales y el estado de emergencia política actual parecen haber hecho caducar los manifiestos como herramientas comunicativas efectivas para los llamamientos a la intervención pública.

La clásica literatura de combate que brota de las emergencias sociopolíticas en forma de manifiesto —descrita por Mangone y Warley (1992)— parecen haber perdido eficacia e interés en nuestra cultura actual. Ya no hay tiempo para manifiestos, como los que anteriormente habían publicado en las décadas de 1980 y 1990 hackers y ciberlibertarios. Así lo reconoce el propio Assange en su llamamiento a las armas criptográficas, en el prólogo de su libro *Cypherpunks: Freedom and the Future of the Internet*: "Este libro no es un manifiesto. No hay tiempo para eso. Este libro es una advertencia" (Assange *et al.*, 2012: 1).

En cuanto a la producción cinematográfica, la popularización de WikiLeaks tras el *Cablegate* activó rápidamente a la industria del cine. Así, por ejemplo, el 2 de marzo de 2011 se estrenó en la séptima edición del festival ZagrebDox el que fue anunciado como primer documental sobre el fenómeno WikiLeaks: *WikiRebels*,

producido por la televisión pública sueca y dirigido por los periodistas Jesper Huor y Bosse Lindquist. Josephson Entertainment y Michelle Krumm Prods se hicieron con los derechos de la biografía *The Most Dangerous Man in the World*, de Fowler, una historia calificada por sus productores como "el drama de suspense de mayor impacto global de esta generación" (Agencias, 2011).

Por su parte, Dreamworks, la productora de Steven Spielberg, compró los derechos de los libros *Wikileaks. Inside Julian Assange's war on secrecy* y *My Time with Julian Assange at the World's Most Dangerous Websit*e, estrenando en 2013 la película *The Fifth Estate*, dirigida por Bill Condon y adaptada por el guionista Josh Singer.

Charles Ferguson, director de *Inside Job,* por el que ganó en 2011 el Oscar al mejor documental, también recibió el encargo de filmar un largometraje sobre Assange para HBO Films y la BBC. Y Alex Gibney fue llamado para dirigir para Universal Pictures un documental sobre el fundador de WikiLeaks, que se estrenó en 2013 con el título *We Steal Secrets: The Story of WikiLeaks*.

Otro interesado en llevar a Julian Assange a la gran pantalla fue el guionista de *En tierra hostil*, Mark Boal, a quien se le encargó un guión basado en el artículo publicado en *The New York Times Magazine* firmado por el exeditor Bill Keller con el título 'Dealing with Assange and the WikiLeaks secrets', extracto del libro del periódico neoyorkino sobre su experiencia con esta organización de filtraciones.

En su país, Australia, la vida de Julian Assange fue llevada al teatro por el dramaturgo Ron Elisha en la obra *Stainless Steel Rat*, anunciada como una *wikiplay* (*wikiobra*). También inspiró un proyecto de la Ópera de Australia liderado por su director artístico Lyndon Terracini y el compositor Jonathan Dreyfus; una obra operística sobre la que Eddie Perfect, quien interpreta a Assange, dijo: "Tiene todo lo que necesita un trabajo musical dramático. Tiene héroes y villanos. De hecho, tiene un héroe y un villano combinados en un mismo personaje" (Trueman, 2011).

También el artista Gennaro Di Virgilio incorporó en 2010 al editor de WikiLeaks como figura central del tradicional Belén que exhibe en su puesto de Milán, en una escena en la que Assange es adorado por los Reyes Magos de Oriente, como si de un mesías se tratase.

Ilustración 43: Belén de Gennaro Di Virgilio con Assange como figura central.

Fuente: http://www.bbc.com/news/world-europe-11952052.

En Internet encontramos toda una suerte de artículos de *merchandising* con la efigie de Assange y montajes fotográficos y audiovisuales creados por usuarios de todo el mundo que lo retratan como el personaje Neo de *The Matrix*, Robin Hood o el Che Guevara, entre otros héroes reales y de ficción (entre los productos que vende la tienda virtual alemana www.getdigital.de hay camisetas con el rostro de Assange y el lema "Viva la info revolución", adaptación del universal "Viva la revolución" que ha acompañado a la fotografía que en 1960 tomó Alberto Korda del Che Guevara, la más reproducida de la historia y símbolo de rebeldía entre generaciones de jóvenes a lo largo y ancho del planeta). "Da la sensación de que la sensibilidad iconográfica del momento ha hallado en la efigie de Julian Assange una poderosa imagen de la revolución de nuestro tiempo" (Muñoz-Rojas, 2011).

Ilustración 44: Meme de Assange convertido en Neo, protagonista de *The Matrix*.

Fuente: https://criticalcitizenry.com/2010/12/09/the-rape-of-julian-assange/.

WikiLeaks también contribuyó a expandir este universo *wiki-rebelde* a través de una tienda virtual con decenas de artículos con su iconografía: camisetas, maletines para ordenadores portátiles, bolsos, gorros, sombrillas, etc., todos sellados con el

logotipo de la organización y lemas y frases populares de Assange. Una estrategia de márketing, con el apoyo del sitio web alemán www.getdigital.de, para que miles de seguidores exhiban por calles de todo el mundo el sello de WikiLeaks, expandiendo el universo WikiLeaks desde el ciberspacio al espacio físico.

Ilusración 45: Tienda *online* con productos de WikiLeaks. Camiseta "Viva la InfoRevolución".

Fuente: captura de pantalla propia tomada de www.getdigital.de.

Lejos de contraerse o de frenarse, el universo WikiLeaks continuó expandiéndose en distintos canales, para distintas audiencias y con distintas narrativas y modos de comunicación. El 17 de abril de 2012, cuando se cumplían quinientos días del bloqueo financiero a WikiLeaks, Julian Assange estrenó en la cadena RT su propio programa de televisión, *The World Tomorrow*. RT es un canal financiado por el Estado ruso que se creó principalmente para promover una imagen positiva de Rusia en el exterior. Como canal transnacional, al estilo Al Jazeera, ofrece emisiones en inglés, español y árabe. A la vez, el programa *The World Tomorrow* tiene su propia página web (http://worldtomorrow.wikileaks.org/) y cada capítulo se difundió también a través del canal en YouTube de RT para alcanzar a una audiencia global. En total, una serie de doce entrevistas a políticos, intelectuales y revolucionarios de todo el mundo para repensar radicalmente el orden establecido desde ideas revolucionarias, algunas de ellas antagónicas. El programa fue coproducido por Quick Roll Productions —empresa fundada por Assange— y Dartmouth Films, productora independiente del Reino Unido;

fue distribuido por la compañía británica Journeyman Pictures y emitido internacionalmente por RT en inglés, árabe y español. Quien fuera declarado *rock star* en 2010 mutó en el año 2012 en estrella y productor de televisión.

La expansión del universo WikiLeaks también se materializó con el lanzamiento de su propia red social *online*. El 20 de mayo de 2012, WikiLeaks explicó oficialmente, en su cuenta en Twitter, su intención de lanzar WLFriends —también llamada FoWL (Friends of WikiLeaks)—, una red social creada para rivalizar con su antagonista natural: Facebook. Aunque su lanzamiento ya había sido anunciado en enero de 2012 y ya se podía proceder a solicitar registro previo a su estreno mediante un formulario, fue el 20 de mayo cuando la organización hizo público que estaba a punto de activar lo que llamó el "Facebook encriptado" de WikiLeaks.

Ilustración 46: WikiLeaks [wikileaks]. (2012, May 20). WikiLeaks 'encrypted Facebook' is almost ready to launch https://t.co/xWcS5ckQ [Tweet]. Recuperado de https://twitter.com/wikileaks/status/204269367100321793

WikiLeaks anunció WLFriends como una red independiente de la actividad de la propia organización que mantendría a salvo los datos de sus usuarios de forma codificada empleando criptografía de grado militar. En su cuenta en Twitter, la organización explicó en doce puntos la esencia de esta red social[186]:

1. WLFriends te pone en contacto con personas que quieres conocer, pero que aún no conoces. Facebook te conecta con gente que ya conoces, lo cual no tiene sentido.
2. Facebook es una herramienta de vigilancia masiva. Tú pones a tus amigos en ella, tú traicionas a tus amigos. ¿Los amigos traicionan a los amigos? WLFriends no conoce a tus amigos. Te presenta nuevos amigos.

[186] Traducción propia. Textos originales disponibles en la cuenta de Twitter de WikiLeaks (https://twitter.com/wikileaks) y en http://www.wikileaks-forum.com/fowl-friends-of-wikileaks/196/why-wl-friends-is-better-than-facebook/11394/ (último acceso: 25 de mayo de 2012).

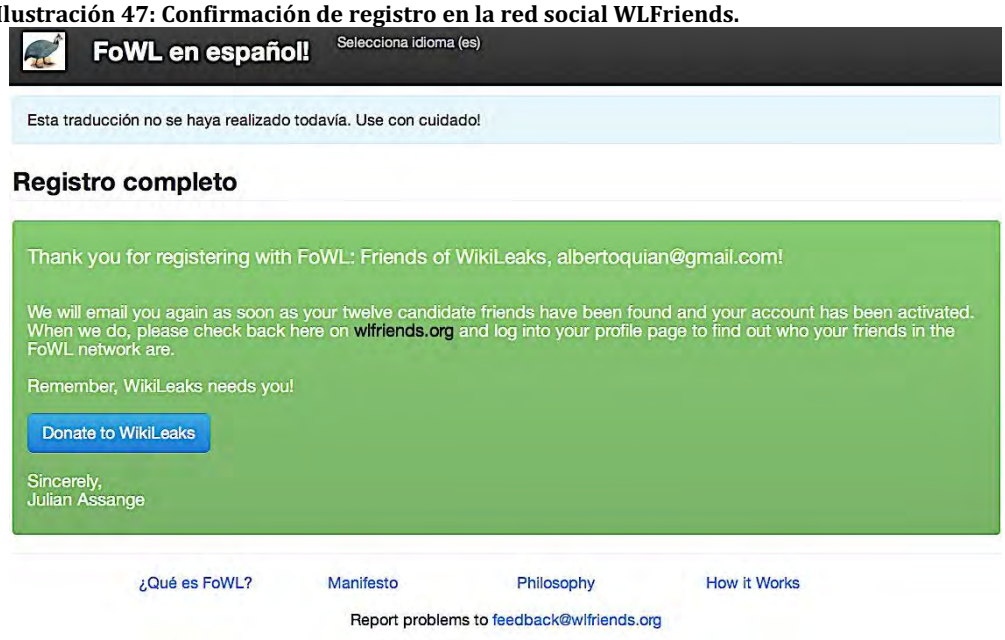
3. Facebook registra todo lo que haces, se lo entrega al Gobierno de Estados Unidos y a las corporaciones. WLFriends no lo hace.
4. WLFriends mantiene tus datos encriptados, ni siquiera los administradores del sistema pueden descifrarlos.
5. WLFriends utiliza criptografía de grado militar y los mejores estándares de la industria (OpenPGP + Elliptic Curves)
6. WLFriends incluso utiliza cifrado homomórfico para ciertas operaciones, de manera que WLFriends no sabe cuántos amigos tienes en esta red.
7. Cuanto más utilices WLFriends, menos lo estarás utilizando. La red está diseñada para construir, no para controlar, una robusta red de valores compartidos.
8. WLFriends está diseñada para algo más que WikiLeaks. Es una solución general para construir una robusta red de apoyo ante condiciones hostiles.
9. Amigos de Israel, de Palestina, del Tea Party, del catolicismo son todos posibles con WLFriends.
10. WLFriends está diseñado para que las infiltraciones sean muy costosas. Ninguna persona puede considerarse más importante que otra o que cualquier objetivo individual.
11. WLFriends construye una fuerte red de apoyo de manera instantánea para cualquier creencia compartida, conectando a partidarios de la misma de un modo que maximiza la comunicación.
12. La red WLFriends para cualquiera causa común ha sido diseñada para que, conforme pase el tiempo, crezca matemáticamente cada vez más fuerte.

    (WikiLeaks, 20 de mayo de 2012)

El 3 de febrero de 2012, procedimos al registro de una cuenta de usuario en esta red social con la intención de escrutar WLFriends y de entrar en contacto con partidarios de WikiLeaks. Fue un ejercicio en vano, ya que WLFriends nunca llegó a ser una red plenamente operativa y fue desactivada finalmente. Entre el 3 de febrero de 2012 y el 25 de enero de 2013 —fecha de la última comunicación que recibimos de WLFriends a través de correo electrónico—, recibimos por correo electrónico un total de diecisiete avisos de esta red social —los dos primeros, firmados por Julian Assange— para: completar y confirmar nuestro registro, el 3 de febrero de 2012; otros dos —uno en inglés el 21 de junio y otro en español el 25 de junio— para avisarnos de que la red estaría pronto plenamente operativa y de que se había actualizado su sistema de seguridad; otro, el 4 de julio para anunciarnos que la red había sido finalmente lanzada el día 2 de ese mismo mes y que se iniciaba el proceso de asignación de amistades basándose en intereses temáticos y áreas geográficas; y el resto de

comunicaciones, hasta el 25 de enero de 2013, para avisarnos de nuevas asignaciones de amistades e informarnos sobre cuestiones relativas a la operatividad de la red, la financiación de WikiLeaks y acontecimientos relacionados con las filtracioes de documentos, a modo de boletín de noticias. En el Anexo III se incluye una muestra representativa de estos correos electrónicos.

Ilustración 47: Confirmación de registro en la red social WLFriends.



Fuente: correo electrónico personal del autor de esta investigación.

IV.8. OBSERVACIÓN PARTICIPANTE: DENTRO DE STRATFOR

IV.8.1. Introducción

Fruto de nuestro registro como periodistas en la red social propia de WikiLeaks —WLFriends—, el 4 de agosto de 2012 recibimos de esta organización una invitación confidencial para unirnos a su grupo de investigación internacional dedicado a los *Global Intelligence Files* (*GI Files*), un inmenso archivo de 5.543.061 correos electrónicos filtrados de la empresa de inteligencia global Stratfor, datados entre julio de 2004 y diciembre de 2011. Esta invitación nos permitió introducirnos dentro del flujo comunicativo de WikiLeaks y, valiéndonos de la metodología de la observación participante, pudimos obtener información fundamental sobre las rutinas productivas operantes en éste.

Nuestra investigación mediante la metodología de observación participante responde a nuestro interés en ofrecer por primera vez una explicación en el campo de la investigación académica sobre los procesos colaborativos y de producción de la noticia en el universo WikiLeaks, en un entorno nuevo, ciberespacial, en el que esta organización opera como proveedor central de información sensible y en bruto almacenada de manera masiva en repositorios virtuales y protegida mediante sistemas de encriptación, antes de su liberación. Alrededor de este nodo central se organiza toda una red ciberespacial de colaboradores que se conectan con éste de manera independiente, principalmente, periodistas, investigadores del ámbito académico y activistas.

A diferencia de lo que sucede en las tradicionales experiencias físicas del investigador que se introduce, observa y/o participa en la vida cotidiana de la gente que está siendo objeto de estudio (Becker y Geer, 1958), nuestra inmersión se produce en un entorno virtual y secreto en el que no existe interacción humana, propiamente dicha. Esta nueva realidad de entornos virtuales, de organizaciones ciberespaciales y de nodos conectados por redes electrónicas nos obliga a redefinir y actualizar las descripciones que sobre la metodología de observación participante han dado diversos autores. Así, por ejemplo, si para McCall y Simmons (1969) es condición *sine qua non* "utilizar una cierta cantidad de interacción auténticamente social" (Elías, 2003: 149), en nuestro caso la interacción social se transforma en interactividad virtual y experiencia unipersonal en una pantalla.

En nuestro caso, la observación se centra en el medio, en los procesos y en los instrumentos y procedimientos con los que se opera en éste, y en los flujos de comunicación e información. Se trata de una observación participante mediada por la virtualidad, en la que las comunicaciones de la otra parte son electrónicas y automáticas —a diferencia de lo que sucedió en las filtraciones de 2010, cuando la interacción humana fue determinante—, donde toda la experiencia del investigador se produce en la pantalla en un proceso de participación y observación en el entorno de trabajo, pero también de autoobservación del propio sujeto investigador, que es a la vez sujeto investigado por sí mismo.

En este entorno ciberespacial, las comunicaciones se producen del nodo central a los distintos nodos de la red WikiLeaks, que reciben los protocolos y herramientas para acceder a un espacio compartido pero protegido, donde cada nodo opera de manera independiente y goza de plena autonomía en el proceso de exploración, selección, producción, publicación y difusión de la información, aunque WikiLeaks impone ciertas condiciones para participar en este proceso, pero sin afectar a la labor de sus colaboradores.

Esta experiencia participativa nos permitió desarrollar la propia labor de investigación, edición y publicación periodística aplicada en complejos procesos de gestión y difusión de enormes volúmenes de información confidencial y secreta, en los que el periodista se enfrenta también a dilemas éticos que contribuyen a comprender mejor la lucha dialéctica entre privacidad y secreto. También nos ayudó a describir las herramientas con las que se opera, los métodos y procesos colaborativos, y la estrategia de gestión y difusión de la información buscando el máximo impacto posible.

A continuación detallamos todo el proceso de nuestra participación en el caso Stratfor: nuestro registro como socios colaboradores de WikiLeaks, los protocolos de seguridad, el acceso a la base de datos, el sistema de archivado, los sistemas de búsqueda de información, la producción periodística y la publicación y difusión coordinada con WikiLeaks de las informaciones que elaboramos a partir de los correos electrónicos y documentos adjuntos encontrados en nuestra fase de exploración de los *Global Intelligence Files*. Y traducimos por primera vez al español comunicaciones y documentos fundamentales que explican los protocolos de colaboración de WikiLeaks.

IV.8.2. Justificación de la elección del medio para publicar los correos y documentos de Stratfor

La elección del periódico digital *Galicia Confidencial* para publicar nuesro trabajo de investigación periodística se debió a varias razones:

1) Porque es un medio con el que el autor de esta tesis ha estado colaborando desde el año 2009 como redactor y como responsable de la planificación, ejecución, control, investigación, monitorización y análisis en redes sociales, y gestión de relaciones con comunidades en línea.

2) Porque es el decano de los periódicos nativos digitales gallegos y referente entre los medios alternativos de Galicia. Fundado en 2003, *Galicia Confidencial* se autodefine como un medio libre de interferencias institucionales y privadas en su línea editorial, en el que se aplica un modelo de periodismo cien por cien independiente, abierto, plural y sostenible, con vocación de servicio público y con una responsabilidad social, gestionado exclusivamente por profesionales de la comunicación y de la información, con el apoyo de expertos informáticos y en colaboración con otros medios y periodistas independientes. Mediante su modelo de periodismo sostenible se busca garantizar la independencia del medio, protegiéndolo de presiones de poderes políticos y económicos. Para ello, se aplica un modelo económico híbrido, con un sistema de financiación pública, mediante donaciones o suscripciones, e ingresos por publicidad que, en ningún caso, deben afectar a la labor de los periodistas y a la independencia del medio.

3) Porque queríamos comprobar si era posible, y de qué manera, integrar y hacer participar a un medio regional en un fenómeno de dimensiones globales, a la vez que buscamos explorar el potencial y la importancia que los fenómenos globales y la liberación masiva de información y de datos, en una sociedad estructurada en red, pueden tener para medios y comunidades locales o regionales. Ligado a estos propósitos, quisimos introducir un idioma regional —el gallego— en la narración de las mayores filtraciones de la historia, cuyo relato ha sido dominado por lenguas internacionales.

4) Porque este medio creó uno de los pocos espejos web en España del sitio de WikiLeaks para "apoyar sus motivos y sus formas" (*Galicia Confidencial*, comunicación personal por correo electrónico, 12 de diciembre de 2010), sumándose así a la red mundial de *mirrors* que protegió a esta organización durante la campaña de acoso que sufrió a raíz del *Cablegate*. El objetivo de esta red de espejos web fue garantizar que los contenidos de WikiLeaks fuesen accesibles, ante los ataques DDoS que sufrió su servidor y el boicot al que fue sometido por sus proveedores de servicios tecnológicos. El *mirror* contenía una réplica exacta del sitio web de WikiLeaks en el servidor de *Galicia Confidencial*, en la dirección: http://wikileaks.galiciaconfidencial.com. Este espejo web se activó el 12 de diciembre de 2010, aunque tuvo que ser temporalmente desactivado dos días después, tras detectarse ataques al servidor de *Galicia Confidencial* relacionados con este *mirror*. Los responsables de este medio gallego también estudiaron por entonces la posibilidad de imitar el modelo WikiLeaks activando "un sistema de «soplos» anónimos, de forma que los «soplones» pudiesen enviar documentos de forma completamente anónima", pero "aunque se encontró la forma de hacerlo", los informáticos decidieron que "no sería efectivo por su complejidad para los confidentes" (*Galicia Confidencial*, comunicaciones personales por correo electrónico, 12 y 14 de diciembre de 2010).

5) Porque es un medio bajo licencia Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0, que permite a cualquiera copiar y redistribuir el material publicado en este periódico en cualquier medio o formato**,** remezclarlo, transformarlo y crear nuevas obras a partir de este material, siempre y cuando no se utilice con fines comerciales, se reconozca adecuadamente su autoría, se proporcione un enlace a la licencia, se especifiquen los cambios realizados —si se ha hecho alguno— y se utilice la misma licencia que en el original. Esta licencia está disponible en: http://creativecommons.org/licenses/by-nc-sa/4.0/.

IV.8.3. Fase 1: Registro y aceptación de términos y condiciones

IV.8.3.1. Introducción

El 4 de agosto de 2012 recibimos la invitación confidencial de WikiLeaks para formar parte del grupo de investigación internacional dedicado a los conocidos como *GI Files*. Hasta ese momento, apenas un uno por ciento de los 5.543.061 de correos electrónicos filtrados de Stratfor habían sido publicados desde el 27 de febrero de aquel año, cuando se anunció esta filtración masiva, la mayor ejectutada por WikiLeaks por volumen de archivos.

Según la propia organización de filtraciones, estos correos revelan el funcionamiento interno de una empresa que actúa como un "editor de inteligencia" que "provee servicios de inteligencia confidenciales a grandes organizaciones, entre ellas, el Departamento de Seguridad Nacional y la Agencia de Inteligencia de Defensa de Estados Unidos" (WikiLeaks Team, comunicación por correo electrónico, 4 de agosto de 2012; Anexo V)[187].

Dada la complejidad de estas filtraciones, con un archivo de más de cinco millones y medio de correos electrónicos imposibles de abordar para los veintinueve medios seleccionados en un principio por WikiLeaks, la investigación y publicación se abrió a más potenciales colaboradores. WikiLeaks creó un sistema de invitación única y confidencial para "periodistas, profesores universitarios y trabajadores de organizaciones de derechos humanos seleccionados para unirse a este proyecto". El sistema permitía a los invitados que aceptasen los 'Términos y Condiciones' de WikiLeaks "obtener acceso inmediato a los archivos con fines de investigación y publicación, e invitar a otras personas dignas de ser incluidas" (WikiLeaks Team, comunicación por correo electrónico, 4 de agosto de 2012)[188]. Es decir, WikiLeaks buscaba ampliar su red de colaboradores para acelerar y extender la publicación de los correos y documentos adjuntos de los *GI Files* que fuesen de interés académico, periodístico y humanitario.

[187] Traducción propia.
[188] Traducción propia.

IV.8.3.2. Instrucciones

La invitación incluía un manual de instrucciones y un código de invitación único para "entrar en un mundo secreto" (Anexo VI)[189]. El equipo de WikiLeaks reconoce que el propósito de este sistema de invitaciones selectivas y confidenciales, para acceder a los correos y documentos adjuntos, es "maximizar el impacto global de los *GI Files*, restringiendo el acceso a aquellas personas con más probabilidades de investigar y publicar sobre éstos" (Anexo VI). Además, los usuarios que demostrasen su "habilidad de investigación y publicación" serían considerados socios para otras publicaciones de WikiLeaks[190] (Anexo VI). A continuación explicamos los pasos a seguir, indicados por WikiLeaks:

1. Tener instalado el navegador web Tor (The Onion Router), herramienta que nos conecta a la red distribuida y de conexiones encriptadas Tor, que garantiza el anonimato y la privacidad de nuestras comunicaciones. Sólo a través de Tor se podía acceder a la página de 'Términos y Condiciones' de los *GI Files* y a su base de datos[191].
2. Ejectutar Tor y dirigirse al siguiente sitio web: http://7f4lihm464gdcwfc.onion/invite/step1 (sólo es operativo usando Tor).
3. Introducir el código de invitación único recibido para tener acceso a los 'Términos y Condiciones' de los *GI Files*.
4. En la página de 'Términos y Condiciones' (Anexo VII), introducir nuestro nombre, el de la organización a la que representamos (en este caso, el periódico *Galicia Confidencial*), una dirección de correo electrónico que no puede ser de uso personal, sino laboral, y un número de teléfono de contacto.

[189] Todas las citas y referencias del documento "GIFiles Signup Instructions", en el Anexo VI, son traducciones propias.
[190] El 12 de septiembre de 2012 recibimos otra invitación de WikiLeaks para participar en la investigación y publicación de los conocidos como *Syria Files*, más de dos millones de correos electrónicos de figuras políticas y ministerios sirios, y de empresas asociadas al Gobierno de este país, fechados entre agosto de 2006 y marzo de 2012 (Anexo IV). Los procesos y procedimientos de invitación, registro, sistema de búsqueda, publicación y difusión son los mismos que en el caso descrito de los *GI Files*. La invitación fue aceptada, pero nos centramos en la investigación de los correos de Stratfor fundamentalmente por dos razones: una, por el enorme esfuerzo que ya suponía para una sola persona explorar, seleccionar, cotejar, verificar, producir y publicar la información obtenida de Stratfor; otra, porque queríamos centrarnos en un caso que era paradigmático para nuestra investigación: la filtración de documentos de una empresa de inteligencia que se dedica al tráfico de información local, regional y global.
[191] Tor se puede descargar en https://www.torproject.org/ (último acceso: 12 de diciembre de 2015).

5. Leer todos los puntos de los 'Términos y Condiciones' y asegurarnos de que entendemos las responsabilidades que debemos asumir.
6. Marcar la casilla de verificación para confirmar el acuerdo.
7. Abrir el mensaje posteriormente recibido en la dirección de correo electrónico proporcionada, con el usuario y clave asignados para acceder a la base de datos de los *GI Files*.
8. Entrar en el sitio de los *GI Files* en la URL http://7f4lihm464gdcwfc.onion/ introduciendo el nombre de usuario y contraseña recibidos. A esta URL solamente se puede acceder mediante Tor.
9. Una vez iniciada la sesión en el sitio web de los *GI Files*, se tiene acceso a la página de usuario, la interfaz de búsqueda y la interfaz de edición.
10. En la página de usuario existen cinco códigos de invitación que se pueden enviar a otros tantos investigadores. Se establecen una serie de condiciones: a) el invitado debe ser una persona real; b) debe ser un periodista, un profesor de universidad o un trabajador de una organización que actúe en defensa de los derechos humanos; c) la organización a la que represente el invitado debe ser diferente a la del usuario que envía la invitación y a las de los otros invitados; d) no debe usar un correo personal; e) el dominio del correo elecrónico de un invitado debe ser diferente al del usuario que envía la invitación y a los de los otros invitados; e) el invitado debe usar sus privilegios como usuario para trabajos de investigación y sus resultados deben ser comunicados al público.
11. Si se viola cualquiera de los 'Términos y Condiciones', la cuenta del investigador y de aquéllos a los que haya invitado pueden ser canceladas.
12. Por último, WikiLeaks ofrece dos canales de chat que se pueden utilizar exclusivamente para resolver dudas sobre este proceso: uno para tratar problemas relacionados con Tor y otro para plantear cuestiones relativas a la base de datos y el trabajo de investigación.

IV.8.3.3. Acuerdo entre las partes

El siguiente paso es el registro y aceptación de los 'Términos y Condiciones' de WikiLeaks para el acceso a los GI Files (Anexo VII). Para ello, accedemos mediante Tor a la página web de 'Terms and Conditions Agreement for GI Files', donde introducimos nuestro nombre, el de la organización a la que representamos y los datos de contacto. Bajo las casillas para el registro se disponen los 'Términos y Condiciones', que constituyen un acuerdo entre nosotros —como individuos, no como organización— y WikiLeaks para el uso de estos archivos[192]:

1. WikiLeaks proporciona el acceso a los *GI Files* a través de la base de datos de WikiLeaks y sus sistema de búsqueda. Ésta debe usarse según las instrucciones del sitio y no pueden utilizarse robots en el sistema.

2. El investigador tiene la potestad exclusiva de decidir qué información se publica en artículos de prensa o académicos, pero deberá atribuir a WikiLeaks el origen de su investigación y reconocer que los documentos han sido obtenidos por esta organización.

3. El investigador debe hacer una referencia clara a los documentos obtenidos por WikiLeaks utilizados en los artículos publicados, y proporcionar un enlace a los datos en la página web de WikiLeaks.

4. Las fuentes de WikiLeaks están sujetas a las protecciones éticas y legales a las que tienen derecho como fuentes confidenciales. De acuerdo con la ética periodística y profesional, no se puede especular sobre sus identidades. En relación con el suministro de información confidencial por parte de WikiLeaks, esta organización debe ser tratada como fuente periodística confidencial. Por lo tanto, aunque el investigador debe reconocer públicamente que la información documental ha sido obtenida por WikiLeaks, no se debe decir que ésta ha sido proporcionada directamente por WikiLeaks, para la protección legal de la propia organización, de sus fuentes y del propio investigador.

5. Antes de publicar cualquier historia o material basado en los *GI Files* el investigador debe informar a WikiLeaks del número de identificación de los

[192] Ofrecemos una traducción propia adaptada del documento original.

datos utilizados en su trabajo, que debe registrar en la plataforma de publicación de WikiLeaks antes de que se publique en cualquier otro sitio, de manera que WikiLeaks pueda liberar los datos originales al mismo tiempo. De esta manera, el investigador se asegura además la exclusividad de su trabajo. El investigador debe proporcionar previamente a WikiLeaks, mediante un sistema de registro, el enlace a la URL del sitio web en la que aparecerá la historia o el material documental, un título descriptivo del contenido y la fecha y hora de publicación programadas. Este sistema de liberación proporcionado por WikiLeaks debe ser tratado con respeto, es decir, no se debe programar la publicación de grandes cantidades de datos con antelación simplemente para reservarse la exclusividad sobre éstos ni se permite el uso de robots en el sistema (para evitar un uso abusivo, el sistema de WikiLeaks sólo permite programar historias con un mes de antelación). Las fechas y horas programadas para la liberación de la información deben cumplirse siempre, para garantizar el buen uso de los datos.

6. El investigador debe tratar los documentos obtenidos de la base de datos de WikiLeaks como confidenciales, a menos que ya hayan sido publicados por otros investigadores o hasta que se liberen. Por lo tanto, el investigador debe proteger la seguridad de esos materiales hasta que sean publicados.

7. Dado que los periodistas de WikiLeaks, empleados, consultores y su propia infraestructura sufren el acecho de las agencias de inteligencia estatales y privadas y un bloqueo financiero, es necesario proteger su capacidad de publicar protegiendo sus identidades y ubicaciones. A menos que se indique lo contrario, esto incluye, pero no se limita a: la identificación de detalles de todo el personal de WikiLeaks, métodos de seguridad, sistemas o métodos de comunicación, localizaciones, planes estratégicos, información sobre amenazas contra WikiLeaks, la cantidad de personal que trabaja para WikiLeaks en diferentes áreas, nombres de usuario, contraseñas o acuerdos financieros, incluyendo métodos de transporte financiero.

8. Está prohibido comerciar con la cuenta de usuario de los *GI Files*. No se puede vender, compartir o transferir la cuenta personal ni vender u ofrecer públicamente las invitaciones.

9. El usuario entiende que cualquier violación de estos 'Términos y Condiciones', o la mala gestión de la base de datos o de la plataforma para liberar los documentos, supone una retirada de los privilegios para acceder a los *GI Files*, tanto para el propio usuario como para cualquier persona que haya invitado. El usuario es responsable de su propia cuenta y de las de las personas a las que invite.

Bajo estos 'Términos y Condiciones' se debe marcar una casilla para confirmar que el investigador se compromete a cumplirlos. Una vez hecho todo esto, se envía el registro al sistema de WikiLeaks, que nos devuelve un correo electrónico de confirmación con el nombre de usuario y contraseña para acceder a la base de datos (Anexo VIII).

IV.8.4. Fase 2: Acceso y exploración

IV.8.4.1. Introducción

Una vez recibidos el usuario y clave asignados, procedemos a ingresar en el sitio web de los *GI Files*. Para ello se nos proporciona una URL que sólo es operativa a través de Tor. En esta página de destino es donde introducimos nuestros datos para obtener el acceso anónimo y encriptado a la base de datos.

Todo el proceso de carga de páginas a partir de aquí es lento debido al sistema de seguridad que se aplica. De media, una página puede tardar hasta diez segundos en cargarse en este sistema, aunque en numerosas ocasiones se demora más, sufriendo incluso algunos cortes temporales en las conexiones, lo que ralentiza aún más el proceso de exploración en una base de datos inmensa como ésta.

IV.8.4.2. Sistema de búsqueda

WikiLeaks pone a disposición del investigador un "sofisticado buscador" (Anexo VI) para encontrar correos electrónicos que coincidan con sus criterios de búsqueda. A continuación describimos sus características.

IV.8.4.2.1. Búsqueda por términos

En la caja de búsqueda podemos introducir cualquier término para obtener correos electrónicos que puedan contener las palabras introducidas, tanto en los campos del remitente, destinatario y asunto del *email*, como en el propio texto de los correos y en los documentos adjuntos. El sistema admite el uso de operadores *booleanos* de búsqueda similares a los que permite Google para refinar las búsquedas. Por ejemplo, se puede usar el signo + entre términos para forzar su inclusión, de manera que sólo obtendremos los archivos que contengan todas las palabras indicadas, o se puede incluir *OR* entre dos términos para que el sistema busque contenidos con una u otra palabra. También se pueden usar caracteres comodines, por ejemplo, el símbolo del asterisco (*) para buscar una cadena de caracteres (si, por ejemplo, introducimos *block**, obtendremos resultados para *block*, *blocked*, *blockade*, *blocking*, etc.).

IV.8.4.2.1.1. Filtros

IV.8.4.2.1.1.1. Filtro por remitente y destinatario

Uno de los filtros que podemos aplicar a las búsquedas por términos es incluir el remitente y/o destinatario de los correos que estamos buscando, de manera que el sistema nos devolverá sólo los documentos que incluyen nuestros términos de búsqueda y que han sido enviados y/o recibidos por cuentas de correo particulares. No es necesario introducir la dirección completa, basta con incluir sólo el nombre identificador (a la izquierda de la arroba y del dominio). Por ejemplo, podemos hacer una búsqueda para la palabra *Spain* e incluir el nombre *Bart* en los cuadros 'Mail from' o 'Mail to' para identificar todos los correos enviados desde o a la cuenta *bart@stratfor.com*[193] referidos a España.

IV.8.4.2.1.1.2. Filtro por el asunto de los correos

Disponemos de una caja llamada 'Subject includes' para limitar la búsqueda de nuestros términos sólo a los correos electrónicos que tienen una determinada palabra en el campo 'Asunto'. Por ejemplo, si hacemos una búsqueda para la palabra *wikileaks* en

[193] Este es un ejemplo ficticio de cuenta de correo electrónico de Stratfor.

el campo general de términos e introducimos la palabra *alfa* en la casilla 'Subject includes', obtenemos sólo los mensajes de correo electrónico que se refieren a WikiLeaks y que contienen la palabra *alfa* en la línea de asunto del correo electrónico. De igual modo, disponemos de una caja 'Subject excludes' que limita los resultados de uno o varios términos de búsqueda a los mensajes de correo electrónico que no tengan una determinada palabra en su campo *Asunto*.

IV.8.4.2.1.1.3. Filtro temporal

Podemos también filtrar contenidos por su fecha de envío, en la caja 'Limit by Date'. Esta opción permite buscar correos electrónicos para uno o más términos limitados a un año concreto, a un mes de un año concreto o a un día concreto de un mes y año determinados.

Todas estas opciones pueden ser combinadas para refinar las búsquedas, pero siempre se debe introducir al menos una palabra en la caja de búsqueda por términos.

Los correos devueltos en la búsqueda pueden ser desplegados en pantalla en grupos de diez, veinte, cincuenta, cien, doscientos, quinientos o mil, agrupados en una página de resultados, y pueden ser ordenados por relevancia, por fecha de publicación (ordenados desde los más recientes hasta los más antiguos, o viceversa) o por orden alfabético de los remitentes (de la A a la Z, o viceversa).

IV.8.4.2.2. Búsqueda por nombre de archivos

El sistema de WikiLeaks ofrece también hacer búsquedas por palabras incluidas en los nombres de los archivos adjuntos a los correos electrónicos. Por ejemplo, si introducimos en este buscador la palabra *payment*, obtenemos todos los correos electrónicos que tienen un archivo adjunto con este término.

IV.8.4.2.3. Búsqueda por ID de documento

Otra opción es buscar un correo electrónico específico por su identificador, si se conoce previamente el ID numérico.

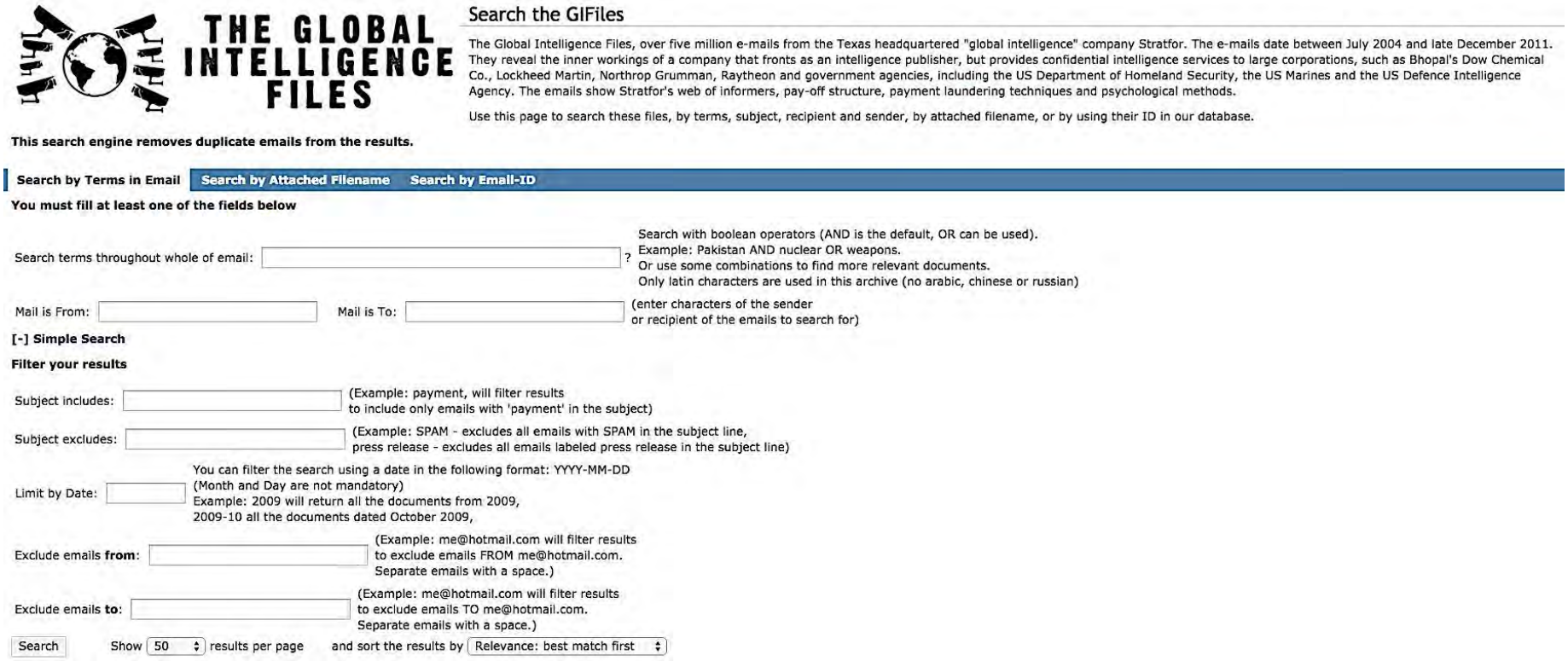
IV.8.4.2.4. Clasificación de los correos

Stratfor clasifica sus correos en grandes grupos mediante códigos incluidos en el campo 'Asunto'. Los encabezados más comunes son: 'OS' (Open-Source), 'Analysis', 'Insight', 'Report', 'Discussion' y 'Question'. La mayoría son fáciles de comprender y son útiles para aplicar filtros en las búquedas. Sin embargo, otros códigos son más limitados en su uso, pero son relevantes, como por ejemplo 'Alpha', utilizado en correos relacionados con las fuentes e informantes de Stratfor en el extranjero, y que pertenecen al departamento de operaciones de la compañía.

En muchos casos, la información relevante se obtiene rastreando las comunicaciones de individuos específicos, por lo que es útil introducir sus nombres y/o direcciones de correo electrónico, pero sin copiar la dirección completa, dado que la función de búsqueda general no reconoce el símbolo @, excepto cuando se introduce la dirección completa de correo electrónico entre comillas.

También es importante destacar que en los correos posteriores al año 2006 las referencias a las fuentes e informantes de Stratfor se hacen con códigos, en lugar de utilizar sus nombres, para proteger sus identidades; por ejemplo: ME213.

Ilustración 48: Buscador para los *GI Files*.



Fuente: captura de pantalla propia.

IV.8.5. Fase 3: Producción, publicación y difusión

IV.8.5.1. Resultados de nuestro trabajo

Fruto de nuestra exploración en la base de datos de los *GI Files*, publicamos once piezas periodísticas entre el 21 de agosto de 2012 y el 20 de mayo de 2013, la mayor parte basadas en correos y documentos relacionados con temas políticos y económicos que afectan directamente a Galicia, aunque también publicamos algunos artículos con contenidos sobre realidades más amplias que fueron exclusivas nacionales o internacionales.

Todas estas investigaciones se basan en correos electrónicos y documentos encontrados en la base de datos de los *GI Files*, aunque también se usaron otras fuentes de información públicas para verificar, contrastar y completar el trabajo periodístico. Resumimos a continuación estas publicaciones por orden cronológico.

IV.8.5.1.1. Publicación 1

- Titular: La mayor compañía de espionaje del mundo vigila el independentismo gallego.
- Fecha: 21 de agosto de 2012.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/11285-maior-compania-espionaxe-mundo-vixia-independentismo-galego.
- Documentos obtenidos en la base de datos de los *GI Files*: correos electrónicos del Departamento de Análisis para Eurasia de Stratfor.

  Resumen: La analista Elodie Dabbagh envía un correo electrónico el 28 de julio de 2010 al Departamento de Análisis para Eurasia de Stratfor con el asunto "[Eurasia] TASKING – Secessionism". Se trata de un breve informe enviado pocos días después de que el Tribunal Internacional de Justicia de la ONU sentenciase que la declaración secesionista de Kosovo, del 17 de febrero de 2008, no había

vulnerado el derecho internacional. Dabbagh inicia su análisis sobre secesionismo en Eurasia con el caso del nacionalismo gallego. La analista se centra en describir la composición del Parlamento de Galicia y la situación de la corriente nacionalista, con mínimas pinceladas sobre el Bloque Nacionalista Galego, del que dice que "desde 1990 fue abandonando el discurso secesionista y las reclamaciones de autodeterminación rara vez se producen". Dabbagh concluye que el movimiento secesionista en Galicia es "muy leve".

- Véase en Anexo IX.

IV.8.5.1.2. Publicación 2

- Titular: Un analista de Stratfor aconsejó hacer un seguimiento a Resistencia Galega.
- Fecha: 27 de agosto de 2012.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/11331-analista-stratfor-aconsellou-facer-seguimento-resistencia-galega.
- Documentos obtenidos en la base de datos de los *GI Files*: correos del Departamento de Análisis de Stratfor e informe de Scotland Yard.
- Resumen: La creciente actividad de Resistencia Galega y la debilidad de ETA hicieron repensar a los analistas de Stratfor la cuestión del terrorismo en España en el año 2011. El 18 de enero, el analista táctico Ben West y la vicepresidenta de Marketing Internacional de la agencia, Antonia Colibasanu, mantuvieron con el departamento de Análisis un intercambio de correos electrónicos sobre las acciones del grupo separatista Resistencia Galega en los que se advertía de amenazas terroristas a cargos políticos en Galicia. Así se expresa en el propio asunto de los *emails*: "Blast targets political office in Spain's Galicia region". West aconsejó hacer un seguimiento al grupo separatista gallego, al que se le atribuían supuestos

vínculos con ETA. Otro informe de Scotland Yard del año 2007 informaba de las acciones de Resistencia Galega. El documento fue creado el 21 de mayo de 2007 por el oficial de Inteligencia Tim Anderson; cinco días después ya circulaba en las comunicaciones privadas de Stratfor. En concreto, estaba en manos de Fred Burton, vicepresidente de Inteligencia de la compañía, quien envió el documento de Scotland Yard a una lista de contactos *vip*, entre los que estaban el director ejecutivo, jefe de Inteligencia y fundador de Stratfor, George Friedman, y Don Kuykendall, presidente de la junta de esta compañía. El documento, titulado *Terror Times*, es un informe del The Metropolitan Police Service Counter Terrorism Command, conocido también como SO15, creado para proteger a Londres y al Reino Unido de la amenaza terrorista. En este informe se incluye una noticia del 16 de mayo de 2006 titulada "Radical separatists claim responsibility for industrial estate bomb", sobre la desactivación por parte de los TEDAX de un artefacto explosivo en el polígono industrial de O Ceao, en Lugo, atribuido a Resistencia Galega, organización a la que también se la responsabilizaba de la colocación, una semana antes, de otro explosivo similar en una obra de construcción en Pontevedra.

- Publicación complementaria: Emails de Stratfor y documento de Scotland Yard sobre Resistencia Galega.
- URL: http://www.galiciaconfidencial.com/nova/11336-emails-stratfor-documento-scotland-yard-resistencia-galega.
- Véase en Anexo X.

IV.8.5.1.3. Publicación 3

- Titular: "El plan en España es que el Santander tome el control como un banco central".
- Fecha: 31 de agosto de 2012.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.

- URL: http://www.galiciaconfidencial.com/nova/11345-plan-espana-santander-tome-control-banco-central.
- Documentos obtenidos en la base de datos de los *GI Files*: correos del Departamento de Análisis de Stratfor.
- Resumen: 30 de sepiembre de 2011. El Banco de España anuncia que el Estado pasa a tomar el control de tres entidades bancarias a través del Fondo de Reestructuración Ordenada Bancaria (FROB) para su recapitalización: el 93 por ciento de NovacaixaGalicia, el 90 por ciento de CatalunyaCaixa y el cien por cien de Unnim. La noticia recorre medio mundo por circuitos financieros y los analistas de Stratfor empiezan a intercambiar correos electrónicos con sus opiniones sobre la nacionalización de las entidades financieras españolas. En uno de esos correos, Peter Zeihan —vicepresidente de Análisis de la compañía— es rotundo en su valoración del sector bancario español: "La mitad es una absoluta mierda" y "la otra mitad, la mejor del mundo". Zeihan, quien cuenta con confidentes en lugares estratégicos como la agencia de calificación Moody's, vaticina por entonces que la debilidad de una buena parte de la banca española condenaría finalmente a España a pedir un rescate e interpreta que "el plan de contingencia español es literalmente hacer que el Santander (la mitad de esa otra mitad [buena]) tome el control como el banco central del país".
- Publicación complementaria: Emails de Stratfor: el plan para el Santander y la «espía» en Moody's.
- URL: http://www.galiciaconfidencial.com/noticia/11375-emails-stratfor-plan-

- **IV.8.5.1.4. Publicación 4**
- Titular: Los negocios sucios del fletador del 'Prestige'.
- Fecha: 13 de septiembre de 2012.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.

- URL: http://www.galiciaconfidencial.com/nova/11470-negocios-sucios-fretador-prestige.
- Documentos obtenidos en la base de datos de los *GI Files*: Informe confidencial *Mikhail Fridman: Background Investigation*.
- Resumen: A un mes del juicio de la catástrofe medioambiental provocada por el hundimiento del petrolero *Prestige* frente a la costa gallega, sucedida el 13 de noviembre de 2002, publicamos un amplio reportaje de investigación elaborado a partir del informe de Stratfor sobre el oligarca ruso Mikhail Fridman, fundador de Alfa Group, consorcio que fletó el buque. Amenazas, sobornos, extorsiones, subastas fraudulentas, tráfico de influencias, tráfico de drogas, prebendas, evasión fiscal, lavado de dinero, violencia y asesinatos brotan cuando se habla de Fridman. El informe de Stratfor, fechado el 2 de agosto de 2007, detalla los negocios e intereses oscuros de un hombre con poderosos vínculos en el Kremlin y relacionado con el crimen organizado, al que los analistas decriben como un individuo "vil". Ni Fridman ni ninguno de sus socios en Alfa Group y su filial Crown Resources fueron juzgados por el vertido de fuel pesado, que contaminó dos mil seiscientos kilómetros de costa. Los responsables de la carga se valieron de artimañas para evitar responsabilidades legales, como se explica en el documento de Stratfor.
- Publicación complementaria: Informe de Stratfor sobre Mikhail Fridman, fletador del 'Prestige'.
- URL: http://www.galiciaconfidencial.com/nova/11510-informe-stratfor-mikhail-fridman-fretador-prestige

IV.8.5.1.5. Publicación 5

- Titular: España ya advirtió del "enorme poder" de Alemania en la UE.
- Fecha: 5 de noviembre de 2012.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.

- URL: http://www.galiciaconfidencial.com/nova/12058-espana-advertiu-enorme-poder-alemana-ue.
- Documentos obtenidos en la base de datos de los *GI Files*: Correos electrónicos entre el consejero para Asuntos Transatlánticos y de Seguridad y Defensa en la embajada de España en Washington y el analista geopolítico Marko Papic.
- Resumen: En marzo de 2010, Camilo Villarino, consejero para Asuntos Transatlánticos y de Seguridad y Defensa en la embajada de España en Estados Unidos, intercambia una serie de correos electrónicos con Marko Papic, analista geopolítico de la agencia de inteligencia Stratfor. En estas comunicaciones el diplomático español advierte de los peligros del nuevo sistema de votación en el Consejo de la Unión Europea, que daría a partir del año 2014 un "enorme poder" a los "cuatro grandes": Reino Unido, Francia, Italia y, sobre todo, Alemania. Las comunicaciones de Villarino con Papic se producen desde su cuenta de correo del Ministerio de Asuntos Exteriores y de Cooperación español, y son firmadas con sus datos oficiales como miembro de la diplomacia española.
- Véase en Anexo XIII.

IV.8.5.1.6. Publicación 6

- Titular: Los negocios de España en la guerra libia.
- Fecha: 10 de enero de 2013.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/12786-negocios-espana-guerra-libia.
- Documentos obtenidos en la base de datos de los *GI Files*: Correos electrónicos entre el consejero para Asuntos Transatlánticos y de Seguridad y Defensa en la embajada de España en Washington y el analista geopolítico Marko Papic, e informe de Stratfor *Special Series: Europe's Libya Intervention*.

- Resumen: El diplomático español Camilo Villarino explica en marzo y abril de 2011, en un intercambio de correos electrónicos con el analista de Stratfor Marko Papic, los intereses y motivos de España y de otros países europeos para participar en la guerra en Libia. Villarino utiliza la cuenta de correo oficial del Gobierno español para comunicarse con el analista de Stratfor. En un amplio informe de esta agencia de inteligencia se detallan también los intereses comerciales y geoestratégicos de los países europeos implicados en la guerra que acabó con el régimen de Muamar el Gadafi en 2011.
- Véase en Anexo XIV.

IV.8.5.1.7. Publicación 7

- Titular: Los intereses europeos en la guerra en Libia.
- Fecha: 14 de enero de 2013.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/12815-intereses-europeos-guerra-libia.
- Documentos obtenidos en la base de datos de los *GI Files*: Informe de Stratfor *Special Series: Europe's Libya Intervention*.
- Resumen: Segunda entrega sobre los intereses de los países europeos en el conflicto libio, en la que se analizan en detalle las estrategias de España, Italia, Reino Unido, Francia y Rusia para obtener beneficios comerciales, políticos y geoestratégicos por su intervención en esta guerra.
- Véase en Anexo XV.

IV.8.5.1.8. Publicación 8

- Titular: ¿Qué pactó el PP con los mercados antes del 20N?
- Fecha: 20 de febrero de 2013.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/13297-pactou-pp-mercados-20n.
- Documentos obtenidos en la base de datos de los *GI Files*: Informe del fondo Emerging Sovereign Group.
- Resumen: El fondo estadounidense Emerging Sovereign Group envía en julio de 2011 un informe a sus clientes en el que se incluyen referencias a un doble discurso del Partido Popular en España antes de las elecciones generales de aquel año, uno para ganarse la confianza de los mercados y otro bien distinto para persuadir a los ciudadanos españoles. En concreto, el informe describe: "La estrategia del PP para ganarse la confianza de los mercados parece ser que es disoponer del expresidente Aznar y contarle a los inversores internacionales en reuniones privadas que un gobierno del PP haría rápidamente recortes presupuestarios y reformas radicales. Al mismo tiempo, Rajoy minimiza en la prensa nacional la posibilidad de tales medidas drásticas, ya que obviamente esto no le permitiría ganar votos".
- Publicación complementaria: El doble discurso del PP sobre recortes y reformas.
- URL: http://www.galiciaconfidencial.com/noticia/13320-dobre-discurso-pp-recortes-reformas.
- Véase en Anexo XVI.

IV.8.5.1.9. Publicación 9

- Titular: Pemex (I): corrupción, crímenes e inseguridad en el nuevo dueño de Barreras.
- Fecha: 9 de mayo de 2013.
- Autor: Alberto Quian.

- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/noticia/14300-pemex-i-corrupcion-crimes-inseguridade-novo-dono-barreras.
- Documentos obtenidos en la base de datos de los *GI Files*: Correos electrónicos de analistas de Stratfor.
- Resumen: Primera entrega de la serie de artículos de investigación y análisis sobre Petróleos Mexicanos (Pemex), la empresa paraestatal que se hizo con control del astillero vigués Hijos de J. Barreras, la mayor factoría naval privada de Galicia. Los correos de Stratfor hablan de graves problemas de seguridad en la empresa mexicana, de corrupción endémica y de estrechos vínculos con el crimen organizado.
- Véase en Anexo: XVII.

IV.8.5.1.10. Publicación 10

- Titular: Pemex (II): opacidad, quiebra técnica y deslocalización de Barreras.
- Fecha: 13 de mayo de 2013.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/14336-pemex-ii-opacidade-creba-tecnica-deslocalizacion-barreras.
- Documentos obtenidos en la base de datos de los *GI Files*: Correos electrónicos de analistas de Stratfor.
- Resumen: Esta pieza informativa se centra en la mala gestión de la compañía paraestatal Petróleos Mexicanos, en la quiebra técnica en la que se encontraba, en irregularidades en las contrataciones, en la polémica y frustrada experiencia de la paraestatal mexicana como accionista de la empresa española Repsol y en su

obsesión por tomar la tecnología de otras empresas. Se explican las claves de la estrategia agresiva de Pemex para intentar llevar el astillero gallego Hijos de J. Barreras a México.

- Véase en Anexo XVIII.

IV.8.5.1.11. Publicación 11

- Titular: Pemex (III): la 'caja chica' de políticos y paraíso de sindicalistas corruptos.
- Fecha: 20 de mayo de 2013.
- Autor: Alberto Quian.
- Medio: *Galicia Confidencial*.
- URL: http://www.galiciaconfidencial.com/nova/14322-pemex-iii-caixa-chica-politicos-paraiso-sindicalistas-corruptos.
- Documentos obtenidos en la base de datos de los *GI Files*: Correos electrónicos de analistas de Stratfor.
- Resumen: Tercera y última entrega de la serie de artículos de investigación y análisis sobre la nueva empresa propietaria del astillero vigués Hijos de J. Barreras. La paraestatal Petróleos Mexicanos es considerada la "caja chica" de políticos corruptos de México. Además, se denuncia que su sindicato recibe millones de euros para dispendios, impone la contratación de sus trabajadores a las navieras privadas y su secretario general es acusado de nepotismo.
- Anexo: XIX.

IV.8.5.2. Programación de las publicaciones

La publicación de informaciones y documentos de los *GI Files* debía ser coordinada con WikiLeaks, según los términos y condiciones del acuerdo de colaboración. Antes de publicar cualquier material, una vez editado y preparado para su liberación, debíamos registrar en el sistema de WikiLeaks la URL donde se publicaría, un título de la información, los identificadores de los correos electrónicos y documentos

utilizados, así como la fecha y hora previstas para la publicación en nuestro medio, de manera que WikiLeaks pudiese también hacer un seguimiento de la publicación y difundirla desde la propia página web de WikiLeaks y desde sus cuentas en Twitter y Facebook. Los pasos a seguir fueron:

1. Ir a la pestaña 'New release' en nuestra cuenta de usuario.
2. En la casilla 'Story name', introducir un título descriptivo y comprensible de nuestra publicación.
3. En el cuadro 'Date and Time of the release', introducir la fecha y hora exacta programadas para la liberar la información.
4. Una vez hecho todo esto, ejecutar la acción 'Create this release'. Hasta que no se realiza, no se pueden introducir los identificadores de los correos electrónicos utilizados.
5. En la casilla 'Story urls' hay que introducir el o los hiperenlaces del sitio web donde se publica la información. De esta manera, WikiLeaks, además de publicar estos enlaces en sus canales de comunicación, asocia las URL a los correos electrónicos, una vez liberados, para que quede constancia de dónde es tratada esa información.
6. En el cuadro 'Email IDs to include in this release', introducir el identificador de los correos electrónicos utilizados en la investigación y ejecutar la acción 'Add this email ID' para incluirlo en la publicación.
7. Tras introducir estos detalles el registro se puede guardar de dos maneras: 1) guardar un borrador en el apartado 'My releases' si es necesario editar más información antes de liberar los documentos, o 2) confirmar y bloquear el registro para su publicación, de manera que ya no podrá ser editado. En este último paso es necesario marcar la casilla 'Ready' y luego ejecutar la función 'Save' para confirmar la programación de la publicación. Una vez hecho esto, el sistema nos confirma la URL pública de WikiLeaks en la que serán liberados los correos y el enlace a la página web donde publicamos nuestra información. También se nos informa si alguno de estos correos ha sido antes confirmado y publicado por otro socio colaborador o si va a ser liberado por otros antes de la fecha y hora programadas por nosotros.

Ilustración 49: Sistema de registro de publicaciones en WikiLeaks.

Fuente: captura de pantalla propia.

IV.8.5.3. Difusión

Todas las piezas informativas se publicaron a la vez en la página web de *Galicia Confidencial* y en la de WikiLeaks, donde nuestro trabajo fue incluido en el registro público de las filtraciones de los *GI Files*.

Ilustración 50: Ficha de nuestro trabajo sobre Mikhail Fridman.

Fuente: captura de pantalla propia.

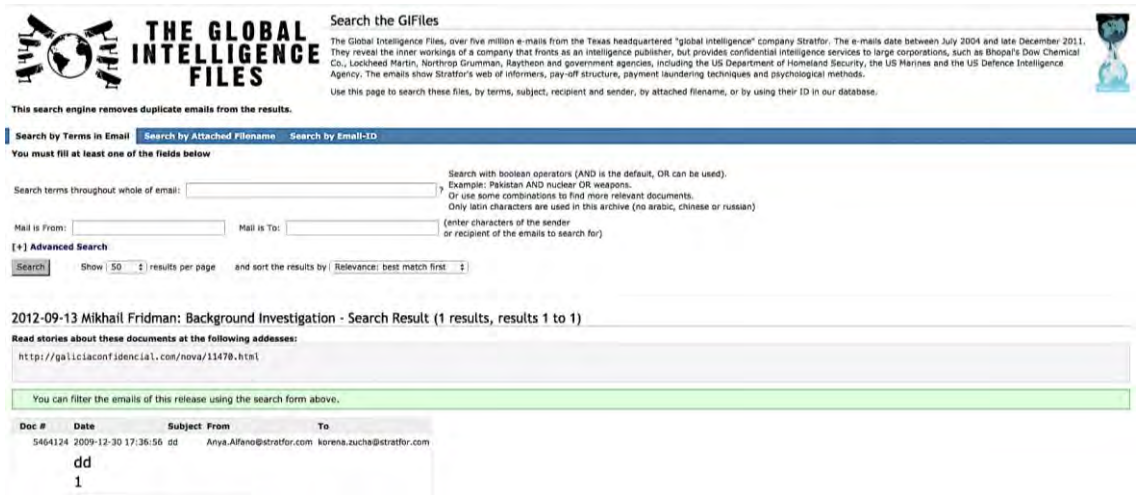
Cuadro 12: Nuestro trabajo sobre Mikhail Fridman, en la lista de los *GI Files* de WikiLeaks.

Barack Obama's Courtship of Bashar al-Assad	2012-09-14
Mikhail Fridman: Background Investigation	2012-09-13
FBI and Stratfor Two Dysfunctional Peas in a Pod	2012-09-12
Greetings - Our govt is capable of anything	2012-09-11
Obama Leak Investigation	2012-09-10
The Hondura's chaos: Fox News and Roger F. Noriega can tell us the Hugo Chavez's secret plan	2012-09-09

Fuente: captura de pantalla propia.

A medida que fuimos publicando nuestras informaciones, WikiLeaks fue liberando en su sitio web los correos electrónicos y documentos adjuntos confidenciales para que cualquier persona pudiese consultarlos en su sitio web. De esta manera, y gracias a su red de colaboradores, WikiLeaks fue creando un gran registro público con la información en bruto (correos y documentos) y enlaces a la información editada que se iba publicando (trabajos de los socios investigadores).

Ilustración 51: Los registros de los correos y documentos en el buscador de WikiLeaks incluyen enlaces a nuestras informaciones.



Fuente: captura de pantalla propia.

WikiLeaks colaboró además en la difusión de nuestros trabajos en las redes sociales en línea. Mientras nosotros hacíamos circular los enlaces por los canales sociales que *Galicia Confidencial* utiliza para difundir sus informaciones, WikiLeaks estaba utilizando paralelamente los suyos para hacer llegar nuestras informaciones a su

comunidad de seguidores en Twitter y Facebook. En sus publicaciones en las redes sociales incluían dos enlaces: uno a la información editada y publicada en *Galicia Confidencial* y otro a la información en bruto liberada en el sitio web de WikiLeaks.

Ilustración 52: WikiLeaks [wikileaks]. (2012, Sep. 15). WikiLeaks: Os negocios sucios do fretador do 'Prestige' http://t.co/0IqSeHw8 http://t.co/mYvBxyrs [Tweet]. Recuperado de https://twitter.com/wikileaks/status/246794427480285184

IV.9. MONITORIZACIÓN DEL IMPACTO DE WIKILEAKS EN INTERNET

A principios de abril de 2010, cuando se publicó el vídeo del asesinato de doce personas desde un helicóptero Apache del Ejército de Estados Unidos en Irak, no era mucha la gente que había oído hablar de Julian Assange y de WikiLeaks. En diciembre de ese mismo año WikiLeaks ya era un fenómeno global, y Assange, uno de los personajes más famosos del planeta, con enemigos muy poderosos y amigos y admiradores muy apasionados (Manne, 2011). El 4 de diciembre de 2010, una semana después de comenzar el *Cablegate* en los cinco grandes medios seleccionados por Assange, la organización se jactaba, a través de su cuenta en Twitter, de ser dos veces más conocida que Wikipedia, de acuerdo con los resultados ofrecidos por Google.

Ilustración 53: WikiLeaks [wikileaks]. (2010, Dic. 04). 'Wikileaks' now twice as known as well known as 'Wikipedia' according to Google. [Tweet]. Recuperado de https://twitter.com/wikileaks/status/11002485711835136

> La consulta de búsqueda en el mismo día confirmó que WikiLeaks devolvió 443 millones de resultados, en contraste con los 208 millones de Wikipedia. La popularidad de WikiLeaks en ese momento no fue una sorpresa, ya que mediante la publicación de una gran cantidad de cables de la diplomacia de Estados Unidos. a través de importantes medios impresos de comunicación seleccionados, se catapultó al centro de atención de la prensa mundial (Barok, 2011: 1)[194].

Los datos obtenidos en nuestra investigación muestran que la coalición de cinco medios tradicionales para el *Cablegate* disparó espectacularmente el impacto y popularidad de WikiLeaks en Internet a finales de noviembre y principios de diciembre de 2010. Luego, a medida que los medios lo fueron relegando o ignorando, fue perdiendo impacto.

[194] Traducción propia.

IV.9.1. Volumen de búsquedas en Google

Para obtener unos primeros datos indicativos del impacto de WikiLeaks en Internet y medir el grado de influencia que los medios de masas tuvieron en su popularidad, utilizamos la herramienta de estadísticas de búsquedas de Google, que recoge el número de búsquedas de un término concreto en comparación con el total de búsquedas realizadas en Google a lo largo de un tiempo determinado, dándonos una medida del interés que suscita un tema. No representan cifras totales del volumen de búsquedas, ya que los datos se normalizan y se presentan en una escala del 0 al 100. Cada punto del gráfico se divide entre el número más alto ó 100. Si no se dispone de datos suficientes, se muestra el valor 0. Como término de búsqueda se introdujo *wikileaks* y se acotó al periodo comprendido entre diciembre de 2006 —cuando se fundó la organización— y marzo de 2012 —tras el inicio de las filtraciones de Stratfor—, para búsquedas en todo el mundo.

Gráfico 11: Evolución de búsquedas de *wikileaks* en Google entre diciembre de 2006 y marzo de 2012.

Fuente: elaboracion propia usando Google Insights.

Los resultados son reveladores. Aunque WikiLeaks ya había filtrado documentos muy comprometedores antes de 2010, no tuvo relevancia en las búsquedas en Google hasta ese año, cuando entabló alianzas con medios convencionales.

El primer pico importante coincide con la publicación en abril de 2010 del vídeo del asesinato de doce civiles en Bagdad. Hasta esa fecha, el valor obtenido en la escala de 0 a 100 fluctuó entre 0 y 1, siendo 0 el más repetido. El 6 abril de 2010, sólo un día

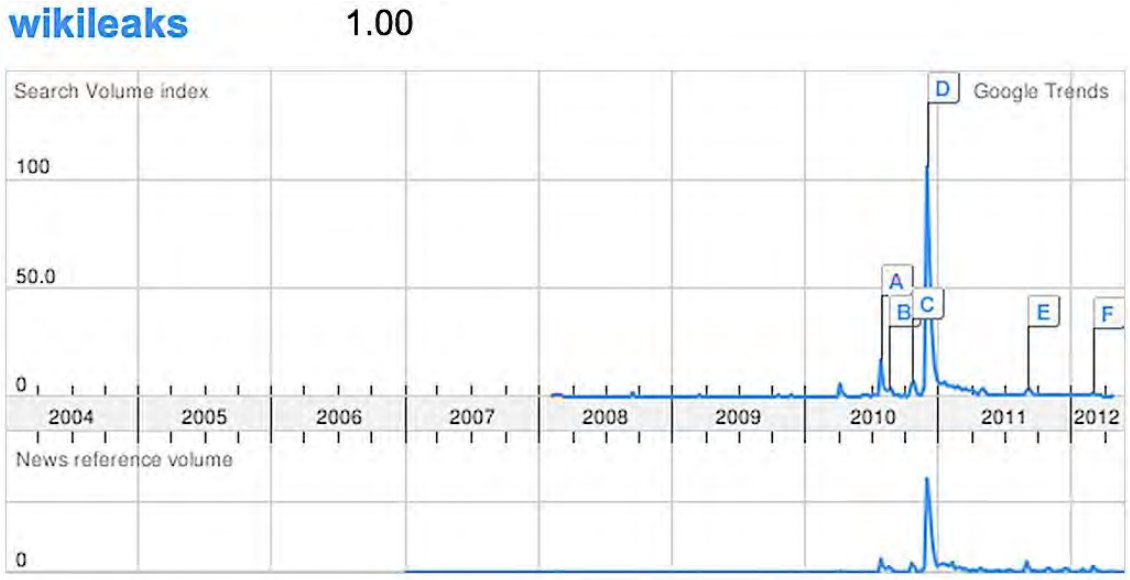
después de presentarse *Collateral Murder* en conferencia de prensa internacional, las búsquedas alcanzaron el valor 5. El segundo mayor pico corresponde al 26 de julio de 2010, cuando logró el valor 11, justo un día después de anunciarse la publicación de los papeles del Pentágono sobre la guerra en Afganistán. La popularidad de WikiLeaks se disparó definitivamente el 23 de octubre, un día después de la conferencia de prensa en la que se anunció la mayor filtración de documentos clasificados de la historia hasta ese momento: 391.832 documentos del Pentágono sobre el conflicto en Irak entre los años 2004 y 2009. Las búsquedas en Google para la palabra *wikileaks* alcanzaron el valor máximo de la escala 0-100 el 29 de noviembre de 2010, justo en el inicio de las publicaciones de los cables diplomáticos estadounidenses. Luego, el número de búsquedas en Google sobre WikiLeaks fue cayendo a medida que las filtraciones fueron pasando a un segundo plano, la atención de los medios se iba centrando en Julian Assange y su relación con los medios se iba deteriorando, aunque el volumen de búsquedas, desde entonces, se mantuvo por encima del registrado hasta abril de 2010.

Entre octubre de 2011 y marzo de 2012 el valor en la escala de Google se mantuvo constante en 2, a pesar de que en diciembre de 2011 se publicaron los *Spy Files* y de que en febrero de 2012 se filtraron los *GI Files* con la colaboración de medios de todo el mundo.

Otra herramienta complementaria a las estadísticas de búsqueda de Google que utilizamos para monitorizar el impacto e influencia de WikiLeaks en la Red fue Google Trends. Esta herramienta nos permitió calcular el número de consultas para la palabra *wikileaks* en relación al número total de búsquedas realizadas en Google en un periodo de tiempo determinado, además del volumen de noticias publicadas en Internet relacionadas con el término de búsqueda.

Como podemos observar en el siguiente gráfico, los resultados que ofrece Google Trends son idénticos a los de Google Insights: el volumen de consultas y de noticias relacionadas con WikiLeaks se dispararon en Internet con motivo de la publicación de los cables diplomáticos de Estados Unidos y, desde entonces, no se volvieron a alcanzar valores semejantes, ni siquiera en febrero y marzo de 2012, cuando WikiLeaks inició la filtración de cinco millones y medio de correos electrónicos de la empresa de inteligencia global Stratfor, en una nueva colaboración con veintinueve medios de comunicación de los cinco continentes.

Gráfico 12: Tendencias de Google con el volumen de consultas y de noticias relacionadas con WikiLeaks.



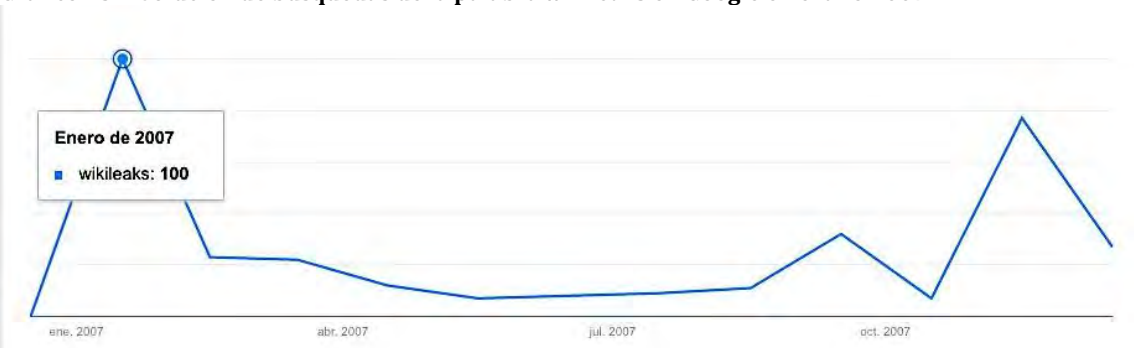
Fuente: elaboración propia usando Google Trends.

Vemos que las búsquedas empiezan a ser algo significativas en el primer trimestre de 2008 y que se disparan coincidiendo con las grandes filtraciones de 2010. Sin embargo, como ya explicamos anteriormente —y como observamos en el gráfico—, las noticias sobre WikiLeaks empezaron a circular por Internet y a ser indexadas por Google desde enero de 2007. Conviene recordar que la revelación prematura de la existencia de WikiLeaks originó una cascada de informaciones en medios en línea[195], alimentada tanto por blogs de reputados e influyentes analistas e investigadores, como por medios especializados y generalistas. "El 15 de enero, Google ya ofrecía 249.000 resultados para la palabra «wikileaks»" (Koman, 2007). Sin embargo, si tomamos el volumen de búsquedas en Google como termómetro del interés suscitado por un tema, observamos que el impacto en la opinión pública en aquel momento fue muy discreto, podemos decir incluso insignificante. Dado que "el volumen de búsquedas no es lo suficientemente elevado para que se muestren resultados" para el término *wikileaks*, según nos dice el propio Google Trends en nuestra búsqueda, nos vemos privados de indicadores sobre el interés geográfico generado por WikiLeaks en sus inicios y de las búsquedas relacionadas que nos permitan conocer qué temas fueron los que más interés suscitaron alrededor de WikiLeaks.

[195] Ir a página 341.

Pero sí podemos constatar que la cascada de informaciones que se publicaron en medios de todo el mundo sobre la aparición de WikiLeaks, en enero de 2007, generó un interés en esta nueva organización que no se repitió a lo largo de ese año. En el siguiente gráfico mostramos el índice de búsquedas entre diciembre de 2006 y diciembre de 2007. El pico más alto se produce en enero y el segundo mayor impacto, en noviembre, cuando WikiLeaks publicó documentos sobre abusos en el centro de detención de la base militar de Guantánamo.

Gráfico 13: Evolución de búsquedas de la palabra *wikileaks* en Google en el año 2007.



Fuente: elaboración propia usando Google Trends.

IV.9.2. Tráfico web

Según los datos de tráfico web recogidos de Alexa.com, de Alexa Internet, Inc. —subsidiaria de la compañía Amazon.com—, la página web de WikiLeaks (http://wikileaks.org/) alcanzó su puesto más alto en el ránking Alexa en diciembre de 2010, colocándose entre los cien primeros sitios de Internet con más tráfico en todo el mundo. Coincidiendo con el inicio del *Cablegate* se registró el mayor porcentaje estimado de usuarios totales de Internet que visitaron el sitio web de WikiLeaks, un 1,7 por ciento, es decir, se calcula que unos treinta y cuatro millones de usuarios visitaron el *site* de la organización en un día[196].

WikiLeaks también alcanzó con el *Cablegate* el mayor porcentaje estimado de páginas únicas vistas por cada usuario en un día: se calcula que hasta un 0,05 por ciento del total de las páginas web visitadas en todo el mundo eran del sitio de WikiLeaks.

[196] A finales de 2010, en el mundo había alrededor de dos mil millones de internautas, según la Unión Internacional de Telecomunicaciones, organismo de la ONU para los asuntos relativos a las tecnologías de la información y de la comunicación.

Gráfico 14: Evolución del sitio wikileaks.org en el ránking de Alexa.

Fuente: captura propia de Alexa.

Gráfico 15: Alcance del sitio wikileaks.org.

Fuente: captura propia de Alexa.

Gráfico 16: Porcentaje de páginas únicas vistas al día del sitio wikileaks.org.

Fuente: capturas propias de Alexa.

IV.9.3. Impacto en Twitter y Facebook

También medimos el impacto de WikiLeaks en Twitter y en Facebook, dos fuentes fundamentales para conocer el impacto mundial de un tema, especialmente la primera, paradigma de la información ubicua y en tiempo real en Internet.

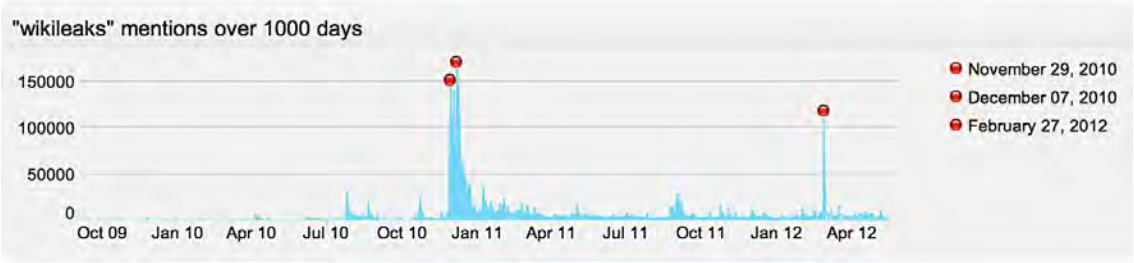
Con Trendistic visualizamos la tendencia de WikiLeaks en Twitter. Los resultados muestran un comportamiento similar al de las búsquedas en Google: WikiLeaks alcanzó su máximo impacto como tendencia en Twitter coincidiendo con las fechas en las que colaboró con cinco medios convencionales en el *Cablegate*.

Gráfico 17: WikiLeaks en el gráfico de tendencias de Twitter.

Fuente: elaboración propia usando Trendistic.

Con PeopleBrowsr contabilizamos el número de menciones diarias a WikiLeaks en Twitter en un periodo de mil días. De nuevo, corroboramos que los niveles más altos, intensos y prolongados de impacto e influencia de WikiLeaks coinciden con el periodo de tiempo en el que se produjo la filtración de los cables diplomáticos de Estados Unidos: entre el 29 de noviembre y el 9 de diciciembre de 2010 se batió el récord de menciones a WikiLeaks en Twitter. Éstas se dispararon también el 27 de febrero de 2012, coincidiendo con el anuncio de la filtración de los correos de la empresa de inteligencia global Stratfor; ese día hubo 107.745 menciones a WikiLeaks.

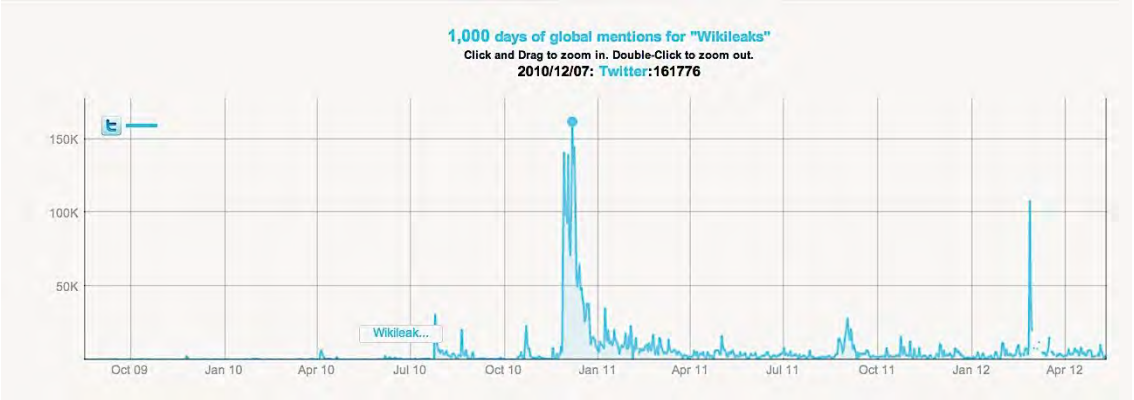
Gráfico 18: Menciones a WikiLeaks en Twitter.



Fuente: elaboración propia usando PeopleBrowsr.

El mayor número de menciones a WikiLeaks en Twitter se produjo el día de la detención de Julian Assange, el 7 de diciembre de 2010; en total, fueron 161.776.

Gráfico 19: Día con más menciones a WikiLeaks en Twitter.



Fuente: elaboración propia usando PeopleBrowsr.

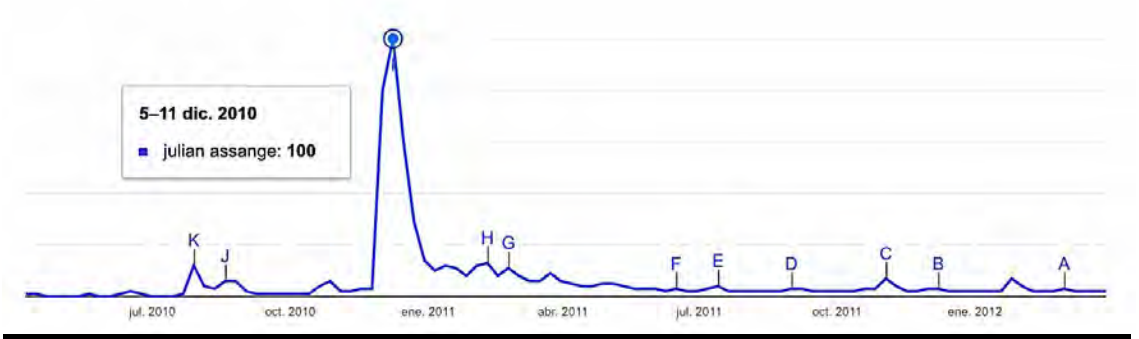
Esta amplificación de WikiLeaks en las redes sociales coincidió también con el mayor volumen de búsquedas sobre Julian Assange en Google.

Gráfico 20: Evolución de búsquedas de 'julian assange' en Google entre diciembre de 2006 y marzo de 2012.

Fuente: elaboración propia usando Google Trends.

Acotando el intervalo de tiempo, entre abril de 2010 —cuando Assange y WikiLeaks empezaron a ser relevantes en las búsquedas de Google— y marzo de 2012, vemos que ese mayor volumen de búsquedas sobre Assange se produjo coincidiendo con su detención y su amplificación en las redes sociales.

Gráfico 21: Evolución de búsquedas de 'julian assange' en Google entre abril de 2010 y marzo de 2012.



Fuente: elaboración propia usando Google Trends.

Observamos más detalladamente en el siguiente gráfico que fue el 7 de diciembre cuando se produjo el récord histórico de búsquedas sobre Assange en Google, día que coincide con el mayor número de menciones en Twitter.

Gráfico 22: Evolución de búsquedas de 'julian assange' en Google en noviembre y diciembre de 2010.

Fuente: elaboración propia usando Google Trends.

A continuación mostramos, ordenados por número de menciones, los días de mayor impacto de WikiLeaks en Twitter y los sucesos que marcaron estas tendencias.

Tabla 4: Días de mayor impacto e influencia de WikiLeaks en Twitter.

FECHA	Nº MENCIONES	ACONTECIMIENTO
7 de diciembre de 2010	161.776	Detención de Julian Assange en Londres. Visa y MasterCard suspenden los sistemas de pagos a WikiLeaks.
9 de diciembre de 2010	144.650	Twitter cancela la cuenta de Anonymous, y Facebook, la página de *Operation Payback*. Amazon sufre ataques DDoS. Lula da Silva defiende a WikiLeaks y la libertad de expresión.
29 de noviembre de 2010	140.816	Día después del inicio de la filtración de 251.287 cables de la diplomacia estadounidense. Assange anuncia que a principios de 2011 prevé difundir material sobre un gran banco norteamericano.
3 de diciembre 2010	139.291	WikiLeaks toma el nombre de dominio suizo WikiLeaks.ch después de que su proveedor estadounidense, EveryDNS, le retire su servicio. Un día antes, la Corte Suprema sueca se niega a examinar el recurso presentado por Julian Assange contra su orden de detención internacional por presuntos abusos sexuales y violación y confirma la orden de captura.
8 de diciembre de 2010	133.102	Ataques DDoS por parte de hacktivistas partidarios de WikiLeaks contra la Fiscalía sueca, la página web de Claes Borgstrom –abogado de las dos mujeres que acusan a Assange de presuntos abusos sexuales– y los servicios de Visa y MasterCard.
27 de febrero de 2012	107.745	WikiLeaks inicia la filtración de cinco millones y medio de correos electrónicos de la empresa de inteligencia global Stratfor, en colaboración con veintinueve medios.
1 de diciembre de 2010	107.363	El jefe de la Comisión de Seguridad Nacional del Senado de Estados Unidos, el demócrata Joe Lieberman, insta a todas las empresas que prestan servicios a WikiLeaks a que finalicen su relación con esta organización. Amazon expulsa a WikiLeaks de sus servidores, en los que se alojaba desde el 29 de noviembre, alegando numerosos ataques informáticos recibidos desde que comenzó la filtración de los cables. Interpol confirma que emitió el 20 de noviembre una Alerta Roja, es decir, una petición internacional de búsqueda y detención contra Julian Assange.

Fuente: elaboración propia con los datos obtenidos con PeopleBrowsr.

Comprobamos que WikiLeaks alcanzó en el inicio del *Cablegate* sus picos máximos de impacto en Twitter: entre el 28 de noviembre y el 9 de diciembre, ambos días inclusive, se hicieron un total de 1.357.984 menciones a WikiLeaks, es decir, una media de 113.165 menciones diarias. En cambio, con las filtraciones conocidas como *The Global Intelligence Files* el impacto fue notablemente menor, a pesar de que WikiLeaks había recurrido a un número mayor de medios colaboradores, repartidos por todo el mundo y culturalmente más diversos. Las filtraciones de la segunda gran alianza de medios de WikiLeaks apenas se mantuvieron un día en niveles similares a los alcanzados con el *Cablegate*, con 107.745 menciones el 27 de febrero de 2012, día que se inició la publicación de los *GI Files*; un día después, se hicieron 40.703 menciones, es decir, una caída del impacto de WikiLeaks de un 62,2 por ciento; en los siguientes días, el *efecto* WikiLeaks se fue diluyendo.

Para medir la influencia y popularidad de WikiLeaks en las dos redes sociales con más éxito, Twitter y Facebook, utilizamos también la aplicación Wildfire App. De Twitter recogimos la evolución del número de seguidores de WikiLeaks y el comportamiento diario, en el periodo máximo de tiempo que nos ofreció esta herramienta: desde el 29 de abril de 2010, cuando WikiLeaks tenía 47.994 seguidores, hasta el 31 de marzo de 2012, cuando sumaba 1.441.757 *followers*.

Los resultados obtenidos muestran que las grandes filtraciones de 2010, coordinadas con varios medios de comunicación globales, dispararon la popularidad de WikiLeaks en las redes sociales. En octubre de 2009, su cuenta en Twitter alcanzó los 10.000 seguidores (Lynch, 2014: 2682); a finales de abril de 2010 prácticamente quintuplicó esa cifra; siete meses después, entre el 28 y el 29 de noviembre, superó los 200.000 seguidores.

En los siguientes gráficos vemos que entre el 28 de noviembre y mediados de diciembre de 2010 se produjo el mayor repunte en el número de seguidores de WikiLeaks en Twitter. El 28 de noviembre de 2010, día en que se anunció la publicación de los documentos del *Cablegate* en los cinco grandes medios coaligados, WikiLeaks tenía 196.195 *followers*; un día después, la organización ya sumaba 238.336 seguidores en esta red (+42.141).

Gráfico 23: Acumulativo del número de seguidores de WikiLeaks en Twitter, entre abril de 2010 y abril de 2012.

Fuente: elaboración propia usando Wildfire App.

Gráfico 24: Evolución del número de seguidores de WikiLeaks en Twitter día a día, entre abril de 2010 y abril de 2012.

Fuente: elaboración propia usando Wildfire App.

El mayor crecimiento de la cuenta de WikiLeaks en Twitter se produjo entre el 28 de noviembre y el 19 de diciembre, pasando de 196.195 *followers* a 573.573 (+377.378), es decir, una media de 17.153 nuevos seguidores cada día. El 31 de diciembre de 2010 la cifra total ascendía ya a 615.068 seguidores (+418.873 desde el 28 de noviembre).

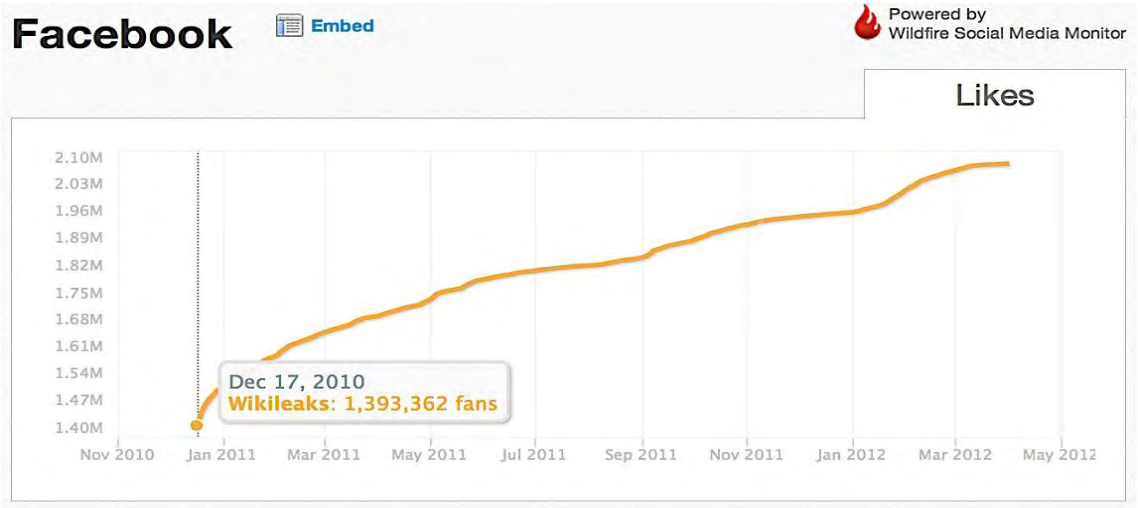
Entre el 28 de noviembre y el 31 de diciembre, WikiLeaks sumó de media 12.693 seguidores cada día en Twitter. Esa tendencia se relajó notablemente a lo largo de 2011 y 2012. El 1 de enero de 2011 contaba con 617.030 seguidores; entre esa fecha y el 31 de marzo de 2012 su cuenta sumó 824.727 nuevos seguidores, con una media de 1.812 nuevos *followers* por día. Debemos destacar también que esta tendencia de crecimiento hizo que WikiLeaks superase el 30 de julio de 2011 el millón de seguidores en esta red social, convirtiéndose en la cuenta número 436 en alcanzar esta cifra, un "caso atípico" —como "grupo radical dedicado a la transparencia informativa"— en el club *millonario* de Twitter (Lynch, 2014: 2679).

El 29 de noviembre de 2010 fue el día que WikiLeaks alcanzó su máximo impacto e influencia, con un récord de 42.141 nuevos seguidores en Twitter. El 27 de febrero de 2012, día que se anunció la publicación de los *GI Files*, la cuenta de WikiLeaks sumó 22.163 nuevos seguidores. A pesar de que en ese momento la organización se había coaligado con veintinueve medios de comunicación de todo el mundo, no alcanzó los mismo niveles de repercusión que tuvo a finales de noviembre y primera semana de diciembre de 2010 gracias a su colaboración con *The New York Times*, *The Guardian*, *Le Monde*, *El País* y *Der Spiegel*. El impacto de la filtración de los correos electrónicos de Stratfor duró apenas un día, coincidiendo con el anuncio mundial de estas publicaciones. Sólo un día después, el 28 de febrero de 2012, WikiLeaks ganó apenas 5.434 seguidores y su impacto fue decayendo progresivamente.

En el caso de Facebook, la herramienta Wildfire App sólo nos ofreció resultados desde el 17 de diciembre de 2010, cuando la cuenta de WikiLeaks sumaba 1.393.362 fans. Pero pudimos comprobar que a partir del 19 de diciembre el número de nuevos seguidores diarios se desplomó, coincidiendo con la progresiva pérdida de interés mediático en las filtraciones de los cables diplomáticos. WikiLeaks no volvió a alcanzar los picos obtenidos en diciembre de 2010, aunque su masa de seguidores no dejó de crecer a un ritmo considerable, al igual que en Twitter.

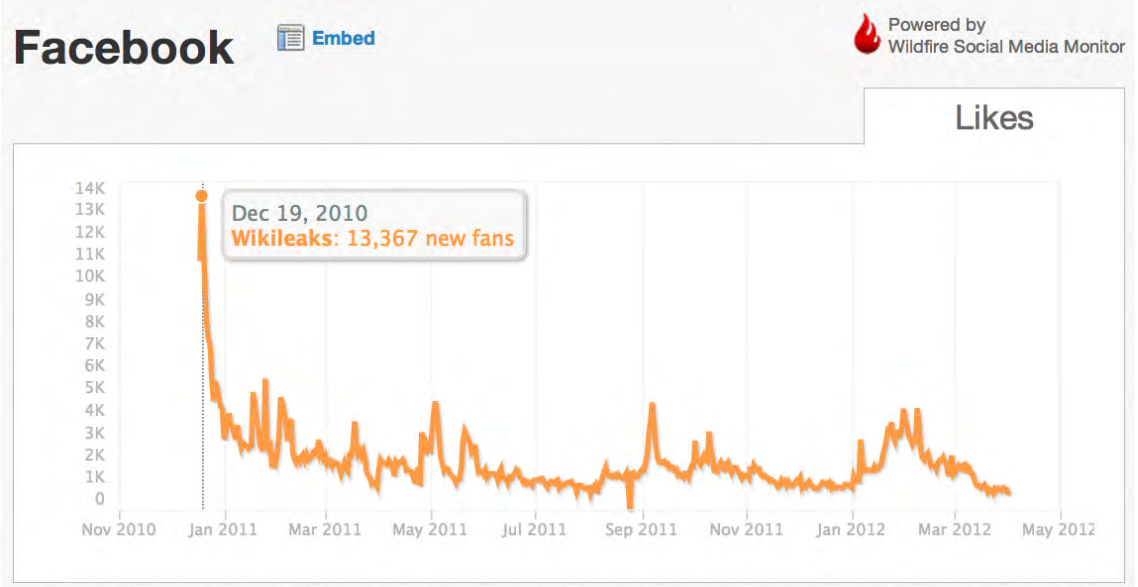
El 1 de enero de 2011, WikiLeaks sumaba 1.493.011 fans en la red social Facebook; el 31 de marzo ya eran 2.070.590 seguidores (+577.579). La media en este periodo de tiempo fue de 1.269 nuevos fans cada día en su página de Facebook.

Gráfico 25: Acumulativo del número de fans de WikiLeaks en Facebook, entre diciembre de 2010 y marzo de 2012.



Fuente: elaboración propia usando Wildfire App.

Gráfico 26: Evolución del número de fans de WikiLeaks en Facebook día a día, entre diciembre de 2010 y marzo de 2012.



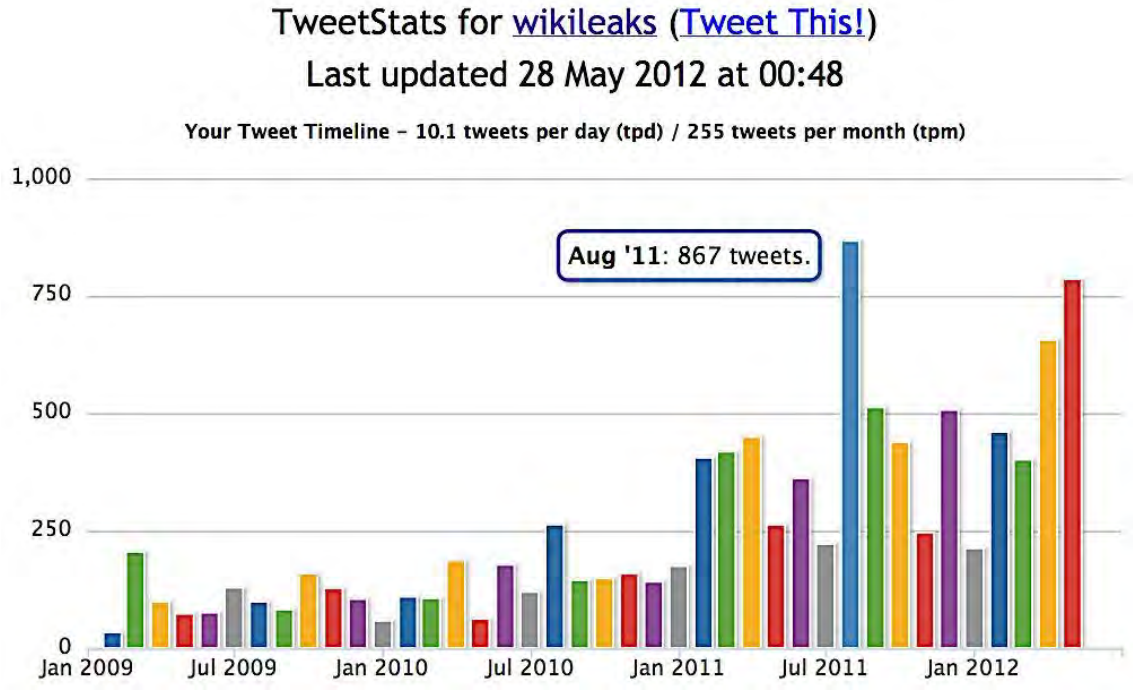
Fuente: elaboración propia usando Wildfire App.

IV.9.4. Actividad de WikiLeaks en Twitter

Para nuestra investigación también era importante obtener datos de la actividad de WikiLeaks en Twitter, pues queríamos comprobar si sus fases de mayor crecimiento e impacto coincidían con periodos de mayor actividad. Para ello usamos la herramienta

TweetStats, con la que obtuvimos la cantidad de *tweets* que WikiLeaks publicó cada mes, entre enero de 2009 y mayo de 2012.

Gráfico 27: Evolución del número de *tweets* publicados cada mes por WikiLeaks en Twitter.



Fuente: elaboración propia usando TweetStats.

Los datos sobre la cantidad mensual de *tweets* publicados por WikiLeaks son reveladores si los comparamos con la evolución del número de seguidores y el impacto que esta organización tuvo en Twitter, y en Internet en general. El cotejo de los datos demuestra que una mayor actividad de WikiLeaks en Twitter no obtuvo como resultado una mayor respuesta por parte de los usuarios. La organización alcanzó su mayor nivel de actividad en las redes sociales en 2011 y 2012. Sin embargo, fue en 2010, coincidiendo con las publicaciones de documentos secretos en cinco de los medios de comunicación tradicionales más influyentes en Occidente, cuando WikiLeaks logró su mayor impacto en Internet y el mayor crecimiento en número de seguidores en redes sociales, alcanzando sus picos máximos durante el inicio del *Cablegate*, a finales de noviembre y principios de diciembre de 2010, cuando su actividad en Twitter era discreta si la comparamos con la que mantuvo durante los años posteriores.

Comprobamos que las publicaciones de WikiLeaks en Twitter fueron *in crescendo* hasta alcanzar sus picos máximos durante 2011 y 2012, a la par que el

impacto de sus filtraciones se iba reduciendo notablemente. En noviembre y diciembre de 2010, en el apogeo del fenómeno WikiLeaks, esta organización *sólo* publicó 159 y 141 *tweets*, respectivamente (una media diaria de cinco). Estos datos contrastan con los 857 *tweets* publicados en agosto de 2011 (una media diaria de casi 28), que coinciden con la polémica sobre la liberación de todos los cables diplomáticos de Estados Unidos sin editar y sin proteger la identidad de las fuentes, presuntamente por un error del que se hicieron eco primero el diario alemán *Der Freitag* y, posteriormente, *Der Spiegel* y *The Washington Post*. Esto llevó a WikiLeaks a responder y defenderse públicamente en su cuenta en Twitter con una serie de mensajes para desmentir a la prensa.

Ilustración 54: WikiLeaks [wikileaks]. (2011, Ag. 29). Current story being spun about wild cables, including from Spiegel, is significantly incorrect. [Tweet]. Recuperado de https://twitter.com/wikileaks/status/108131963898052610

Ilustración 55: WikiLeaks [wikileaks]. (2011, Ag. 29). WikiLeaks 'insurance' files have not been decrypted. All press are currently misreporting. There is an issue, but not that issue. [Tweet]. Recuperado de https://twitter.com/wikileaks/status/108251897961517056

Ilustración 56: WikiLeaks [wikileaks]. (2011, Ag. 29). There has been no 'leak at WikiLeaks'. The issue relates to a mainstream media partner and a malicious individual. [Tweet]. Recuperado de https://twitter.com/wikileaks/status/108261633859649536

Fuente: Capturas de pantalla de la cuenta de WikiLeaks en Twitter.

IV.9.5. WikiLeaks en Wikipedia: interés generado

Por último, recuperamos las estadísticas generadas por el artículo dedicado a WikiLeaks en Wikipedia, como principal fuente secundaria de información en Internet sobre esta organización y termómetro del interés que puede suscitar un tema.

Ilustración 57: Primeros resultados de búsqueda para la palabra *wikileaks* en Google.

Fuente: captura de pantalla propia tomada de Google.com.

Coincidimos con Snickars (2014: 2668) en que esta página de la enciclopedia libre puede ser tomada como un archivo de una conversación popular en curso sobre WikiLeaks, ofreciéndonos un marco para la comprensión de cómo es seguida y entendida esta organización, al preservar datos históricos e información relevante del discurso popular sobre ésta. En nuestro caso, el objetivo era analizar la actividad que genera esta página, tanto la relativa a las ediciones, es decir, a la producción del contenido, como a las consultas de los usuarios de Internet.

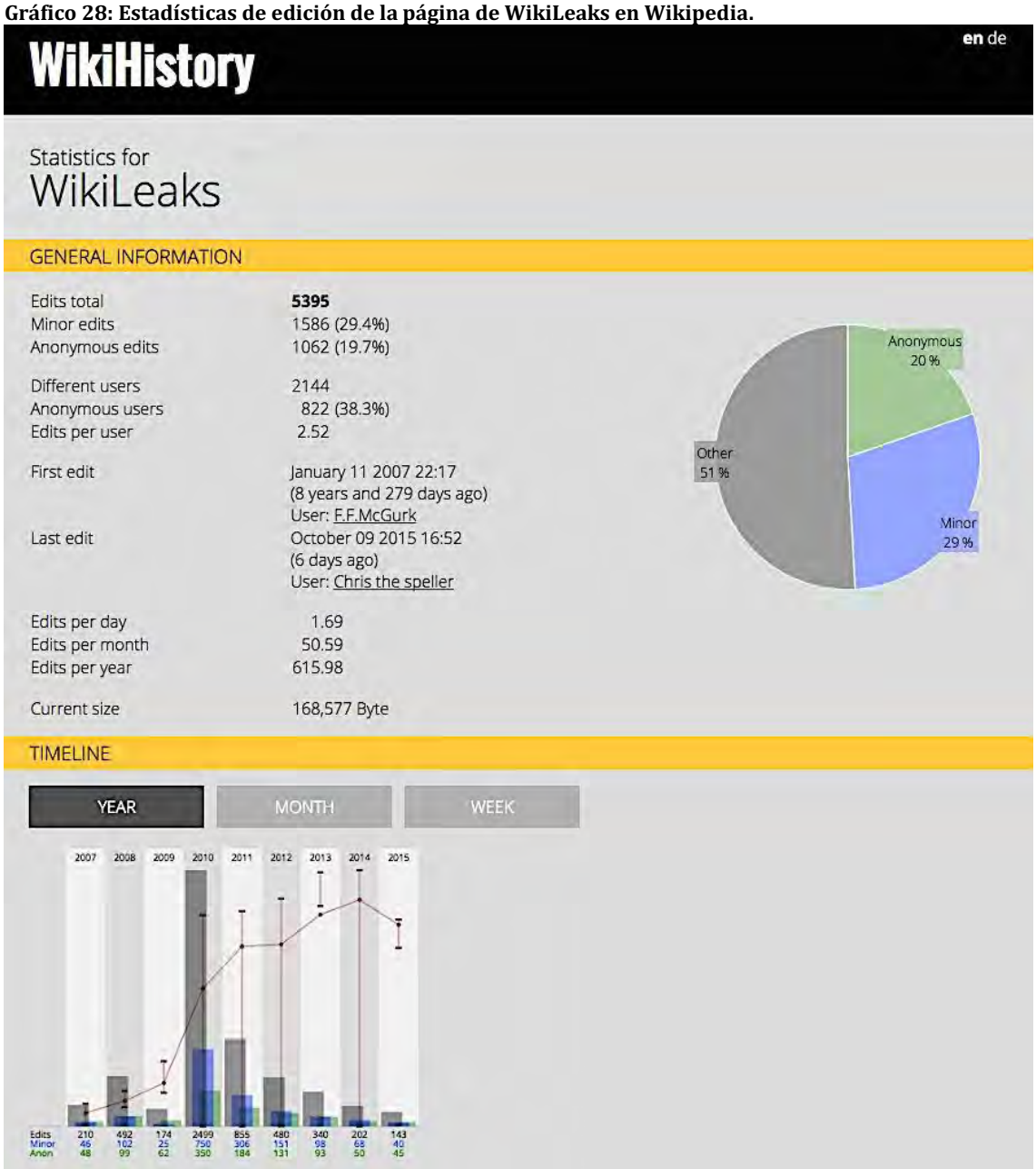
Lo que pretendemos con los datos de edición y tráfico de este *wiki* es completar la evaluación del interés que genera el fenómeno Wikileaks en la Red y comprobar si los periodos de máxima actividad en esta página de Wikipedia coinciden también, o no, con los momentos de máximo impacto mediático de WikiLeaks y su máxima actividad en las redes sociales y búsquedas en Google.

Para nuestro análisis seleccionamos la versión en inglés del *wiki* de WikiLeaks —https://en.wikipedia.org/wiki/WikiLeaks— por ser la principal fuente de información y la página que más acciones genera entre los usuarios y visitantes de Wikipedia que editan y buscan información sobre esta organización. Además, decidimos confrontar los datos generados por la página de WikiLeaks con los de los *wikis* de Facebook y *The New York Times*, para comparar el interés que WikiLeaks y sus dos antagonistas mediáticos más paradigmáticos suscitan entre los usuarios de la enciclopedia libre.

Primero, aportamos estadísticas de edición de los tres *wikis* y, posteriormente, ofrecemos datos sobre el tráfico a la página de WikiLeaks en Wikipedia.

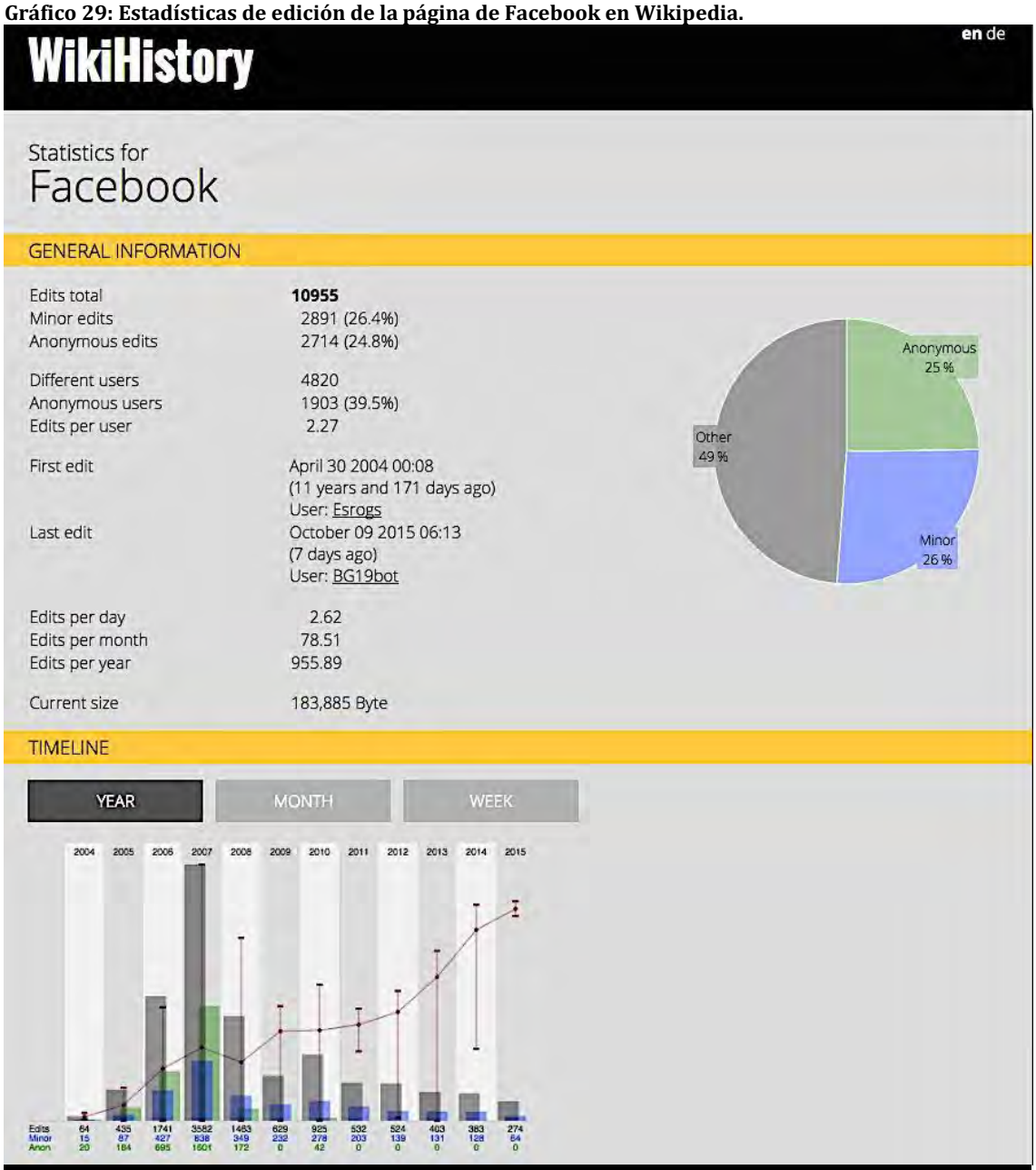
Los siguientes gráficos fueron obtenidos de Wikipedia el 16 de octubre de 2015 y muestran el historial de ediciones de las páginas de WikiLeaks, Facebook y *The New York Times*.

Gráfico 28: Estadísticas de edición de la página de WikiLeaks en Wikipedia.



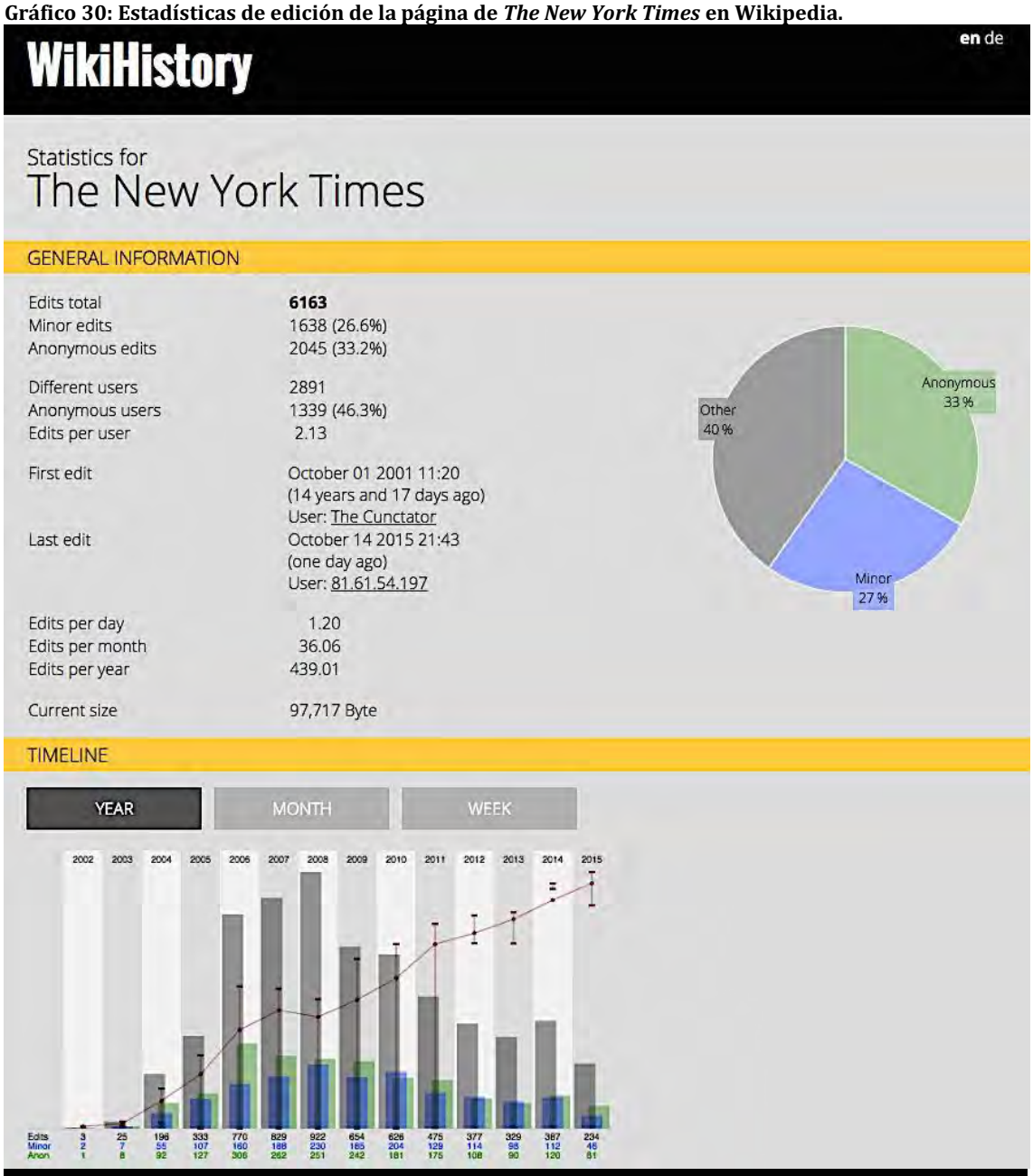
Fuente: captura de pantalla propia tomada de https://tools.wmflabs.org/xtools/wikihistory/wh.php?page_title=WikiLeaks (acceso: 16 de octubre de 2015).

Gráfico 29: Estadísticas de edición de la página de Facebook en Wikipedia.



Fuente: captura de pantalla propia tomada de https://tools.wmflabs.org/xtools/wikihistory/wh.php?page_title=Facebook (acceso: 16 de octubre de 2015).

Gráfico 30: Estadísticas de edición de la página de *The New York Times* en Wikipedia.

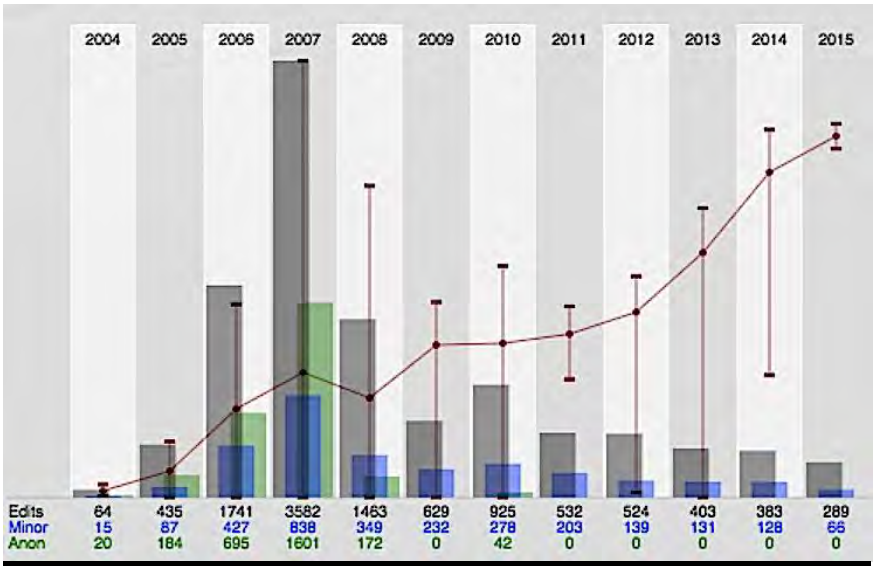


Fuente: captura de pantalla propia tomada de https://tools.wmflabs.org/xtools/wikihistory/wh.php?page_title=The_New_York_Times (acceso: 16 de octubre de 2015).

El primer dato relevante que encontramos es la fecha de creación del *wiki* de WikiLeaks, el 11 de enero de 2007, sólo ocho días después de que la existencia de esta organización fuese prematuramente revelada y de que se iniciase una reacción mediática en cadena. Esta rapidez con la que se creó la página de WikiLeaks en Wikipedia nos da una idea del interés inmediato que suscitó la aparición del sitio de filtraciones en la nueva esfera pública.

Si tomamos el promedio diario de ediciones de cada página de Wikipedia como un indicio del interés que genera un tema entre los editores de esta enciclopedia libre, vemos que Facebook (2,62 ediciones/día) supera con creces a WikiLeaks (1,60), que a su vez aventaja a *The New York Times* (1,20). De estos datos podríamos deducir que Facebook es una empresa que genera más cantidad de información y más constante, lo que obliga a los editores de Wikipedia a actualizar de manera máis intensiva su *wiki*. Sin embargo, si observamos la evolución histórica de ediciones en cada una de estas tres páginas podemos constatar que el promedio de ediciones en el *wiki* de Facebook se dispara en el año 2007, con un total de 3.582 modificaciones, con una marcada tendencia a la baja desde entonces.

Gráfico 31: Evolución de las ediciones en el *wiki* de Facebook.

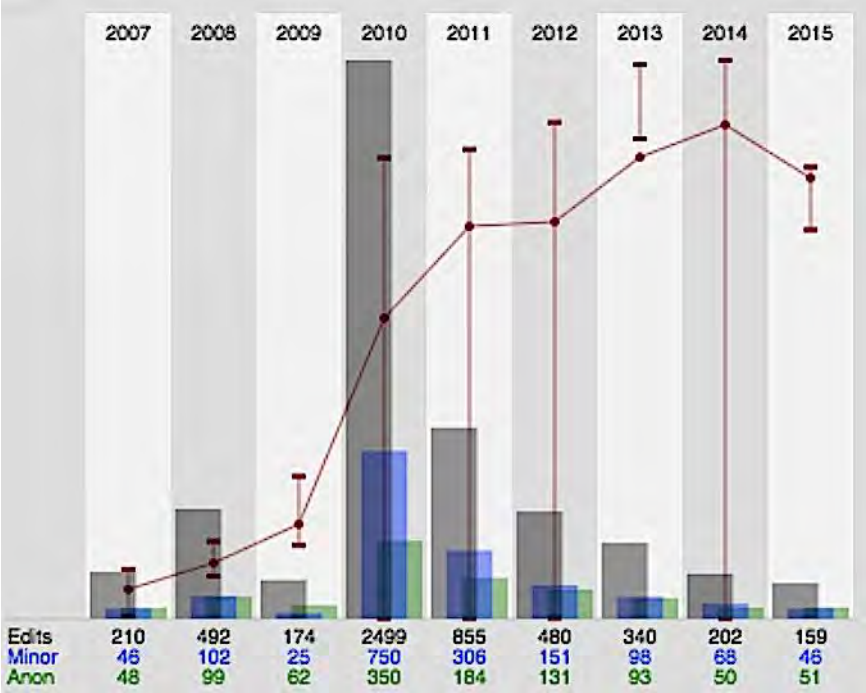


Fuente: captura de pantalla propia tomada de https://tools.wmflabs.org/xtools/wikihistory/wh.php?page_title=Facebook (acceso: 16 de octubre de 2015).

La explicación a este comportamiento la encontramos en la enorme expansión social y económica que Facebook experimentó en 2007. Aquel año, se convirtió en la segunda red social más popular del mundo —sólo por detrás de MySpace—, alcanzando los cincuenta millones de usuarios; además, se estrenaron las páginas para empresas y organizaciones, la publicidad empezó a invadir esta red social y Microsoft pagó 240 millones de dólares por una participación del 1,6 por ciento en su capital, valorando Facebook en 15.000 millones de dólares.

En el caso de WikiLeaks, observamos un comportamiento similar en la evolución de las ediciones en su página de Wikipedia: la actividad de los editores se disparó en el año 2010, con un total de 2.499 modificaciones, cuando esta organización se dio a conocer globalmente con las filtraciones masivas de documentos secretos de Estados Unidos, situándose en el centro del debate político mundial.

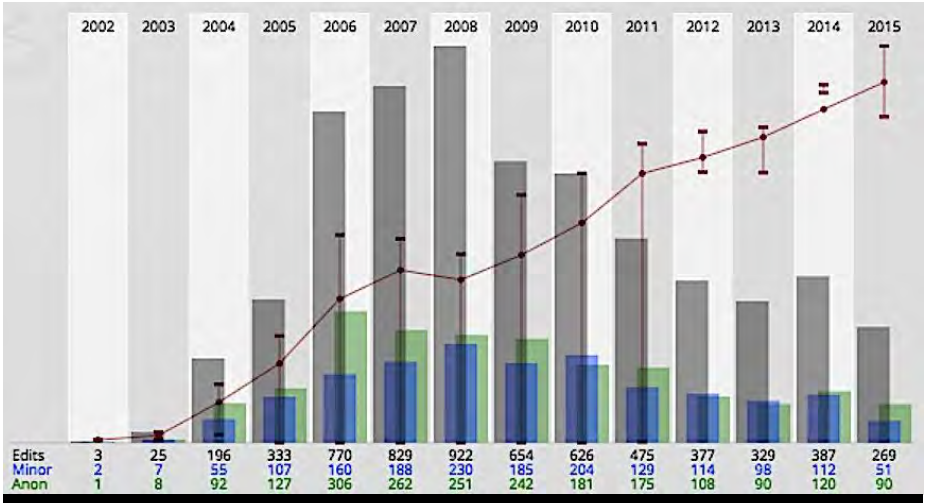
Gráfico 32: Evolución de las ediciones en el *wiki* de WikiLeaks.



Fuente: captura de pantalla propia tomada de https://tools.wmflabs.org/xtools/wikihistory/wh.php?page_title=WikiLeaks (acceso: 16 de octubre de 2015).

En las ediciones de la página del periódico *The New York Times* vemos un comportamiento más estable, sin fluctuaciones tan grandes, y menos intenso que en los casos de Facebook y WikiLeaks, que, como fenómenos globales y populares, parece que requieren más actualizaciones vinculadas a acontecimientos de gran impacto social.

Gráfico 33: Evolución de las ediciones en el *wiki* de *The New York Times*.



Fuente: captura de pantalla propia tomada de https://tools.wmflabs.org/xtools/wikihistory/wh.php?page_title=The_New_York_Times (acceso: 16 de octubre de 2015).

Otra variable cuantitativa relevante es el número de usuarios distintos que participan en la edición de estas páginas. Cuanto mayor es este número, se deduce que mayor es el interés que genera un tema entre la comunidad de editores de Wikipedia. Pero el número total debe ser tomado con precaución. Para estimar el poder de atracción de editores calculamos la relación entre la cantidad total de usuarios que han editado una página y el tiempo total que ese tema lleva publicado, para hallar el promedio diario de editores que atrae cada página, siendo 1,06 para la de Facebook; 0,60 para la de WikiLeaks, y 0,52 para la de *The New York Times*.

También nos parece significativo el promedio de ediciones por usario en cada *wiki*, siendo de 2,52 en el caso de la página de WikiLeaks, 2,27 en la de Facebook y 2,13 en la de *The New York Times*, de lo que inferimos que los editores del *wiki* de WikiLeaks son más activos y están más comprometidos y preocupados por corregir, mejorar y enriquecer su contenido.

El número de *bytes* acumulados en cada *wiki* —es decir, su tamaño— nos sirve también para comparar el volumen de datos e información que contiene cada página y, de esta manera, determinar qué temas son más elaborados. Así, vemos que la página de Facebook es la de mayor tamaño, con 183.885 *bytes*; la de WikiLeaks tiene un peso similar, con 168.577 *bytes*, y mucho más pequeña es la de *The New York Times*, con 97.717 *bytes*.

Por último, introducimos otra variable cuantitativa que nos parece relevante en nuestro intento por evaluar el interés que despiertan estos *wikis* entre la comunidad de Wikipedia. Se trata del número de vigilantes de estas páginas, es decir, los usuarios registrados que mediante un sistema de alertas hacen un seguimiento de los cambios realizados en estos *wikis* y en las páginas de discusión asociadas a éstos. En términos absolutos, la expectación que generan las modificaciones en la página de Facebook es mucho mayor que la que suscitan las de WikiLeaks, que a su vez casi dobla a la de *The New York Times*.

Tabla 5: Usuarios que vigilan los cambios de los *wikis* de WikiLeaks, Facebook y *The New York Times*.

Wiki	Número de vigilantes
WikiLeaks	751
Facebook	1.858
The New York Times	403

Fuente: elaboración propia a partir de los datos obtenidos el 16 de octubre de 2015 de:

https://en.wikipedia.org/w/index.php?title=WikiLeaks&action=info#mw-pageinfo-watchers.

https://en.wikipedia.org/w/index.php?title=Facebook&action=info#mw-pageinfo-watchers.

https://en.wikipedia.org/w/index.php?title=The_New_York_Times&action=info#mw-pageinfo-watchers.

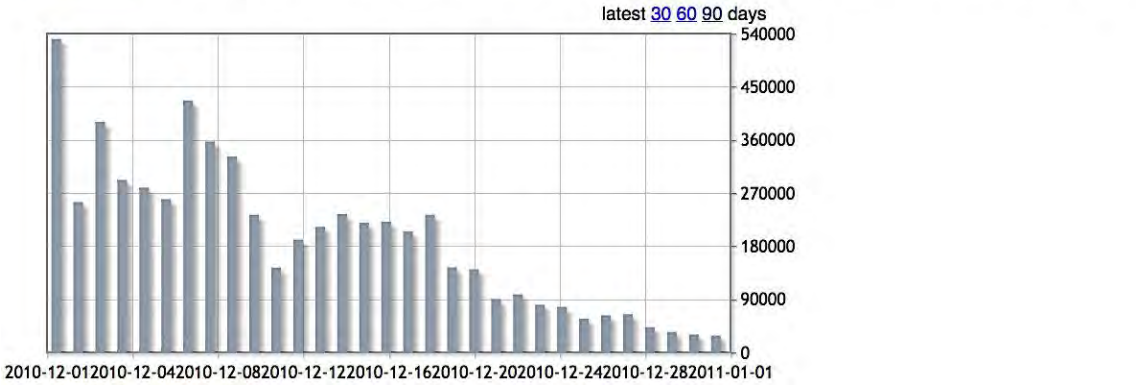
Pero si calculamos el porcentaje de editores de cada *wiki* que son vigilantes, obtenemos datos similares para Facebook y WikiLeaks: en el primer caso representan el 16,96 por ciento del total y en el segundo, el 13,92, mientras que en el de *The New York Times* sólo son el 6,54 por ciento. De esto inferimos que fenómenos globales y populares generan mayor expectación y compromiso en los editores de Wikipedia.

Finalmente, recogimos las estadísticas de visitas a la página de WikiLeaks en Wikipedia en los periodos de tiempo de mayor actividad, que, como vamos a ver, coinciden con la mayor exposición de WikiLeaks y de Julian Assange en los medios de comunicación de masas y en las redes sociales.

Los gráficos fueron obtenidos del servico público de estadísticas Stats.Grok.se, que ofrece datos de visitas de cada página de Wikipedia, mostrándonos la relevancia que los *wikis* tienen como fuente de información para los internautas que siguen acontecimientos de actualidad, en este caso, los relacionados con WikiLeaks.

En consonancia con los datos de las búsquedas en Google y del impacto en redes sociales, también fue en diciembre de 2010 cuando el fenómeno WikiLeaks alcanzó su apogeo en Wikipedia, frisando seis millones de consultas en total.

Gráfico 34: Evolución de visitas a la página de WikiLeaks en Wikipedia en diciembre de 2010.



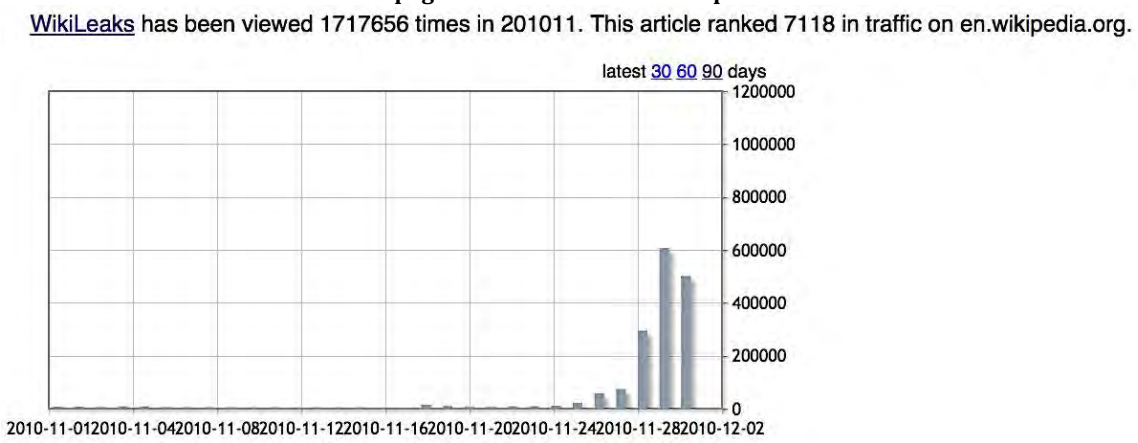
Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

El día que más visitas recibió el *wiki* de WikiLeaks fue el 1 de diciembre de 2010, con 530.832 consultas, coincidiendo con la petición del jefe de la Comisión de Seguridad Nacional del Senado de Estados Unidos, Joe Lieberman, a las empresas que prestaban servicios a WikiLeaks para que finalizasen su relación con esta organización, la expulsión de la página web de WikiLeaks de los servidores de Amazon y la confirmación de Interpol de la Alerta Roja para la detención de Assange.

El segundo día de mayor actividad en la página de WikiLeaks en Wikipedia en diciembre de 2010 fue el 7 de diciembre, con 426.565 visitas, coincidiendo con la detención de Julian Assange en Londres.

Pero el día que el *wiki* de WikiLeaks alcanzó su máximo histórico de visitas fue el 29 de noviembre de 2010, justo en el inicio del *Cablegate*, cuando se alcanzaron las 607.161 consultas, esto es, el 35,35 por ciento del total de las visitas registradas durante el mes de noviembre, el segundo más activo en el registro histórico de esta página, con un total de 1.717.656 consultas.

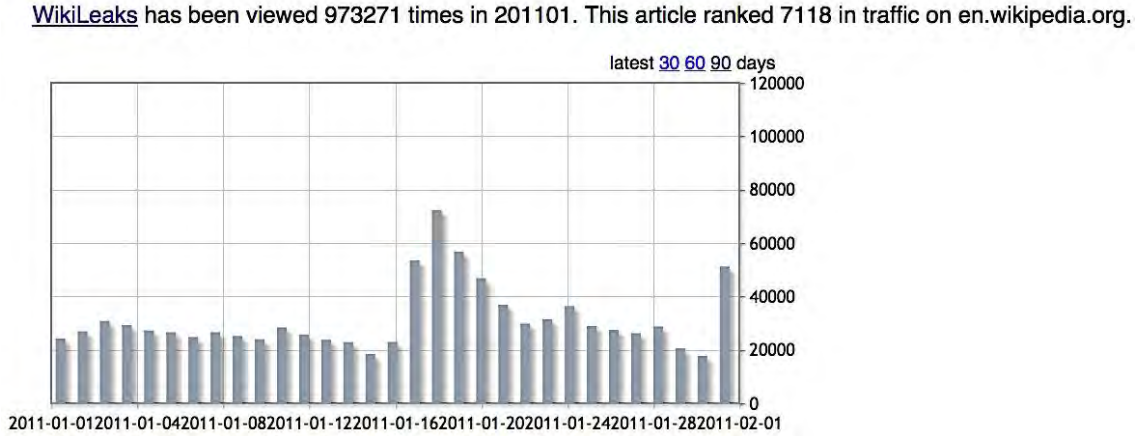
Gráfico 35: Evolución de visitas a la página de WikiLeaks en Wikipedia en noviembre de 2010.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Los coletazos del *Cablegate* y de la detención de Assange aún se sintieron en Wikipedia en enero de 2011, mes en el que se registraron casi un millón de consultas al *wiki* de WikiLeaks, con el pico más alto el día 18, con 72.369 consultas. Nunca antes de noviembre de 2010 ni después de enero de 2011 se alcanzaron cifras similares a las conseguidas en el inicio del *Cablegate*.

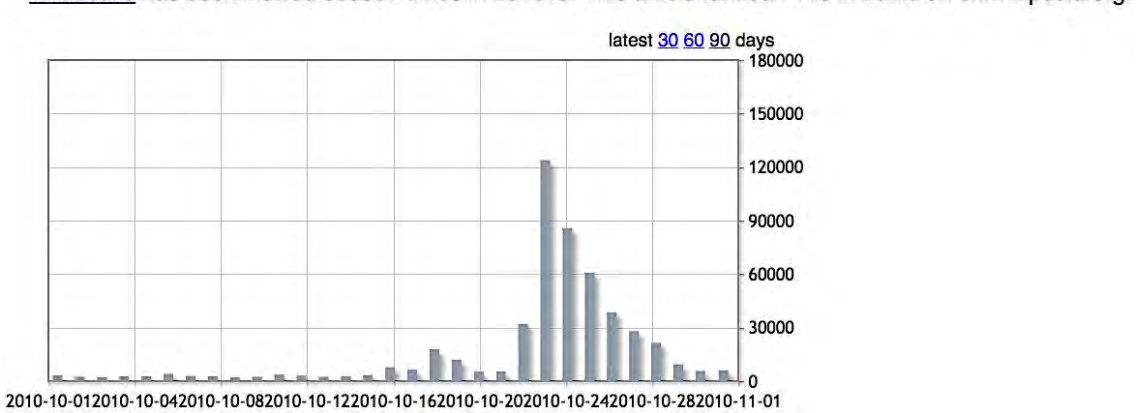
Gráfico 36: Evolución de visitas a la página de WikiLeaks en Wikipedia en enero de 2011.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Retrocediendo en el tiempo comprobamos que el impacto de WikiLeaks va descendiendo. En octubre de 2010, el total de consultas ascendió a 509.307, siendo el día 23 el de mayor actividad, con 123.896 visitas, cuando se disparó la popularidad de WikiLeaks, un día después de anunciarse en coferencia de prensa la publicación de 391.832 documentos filtrados del Pentágono de la guerra en Irak.

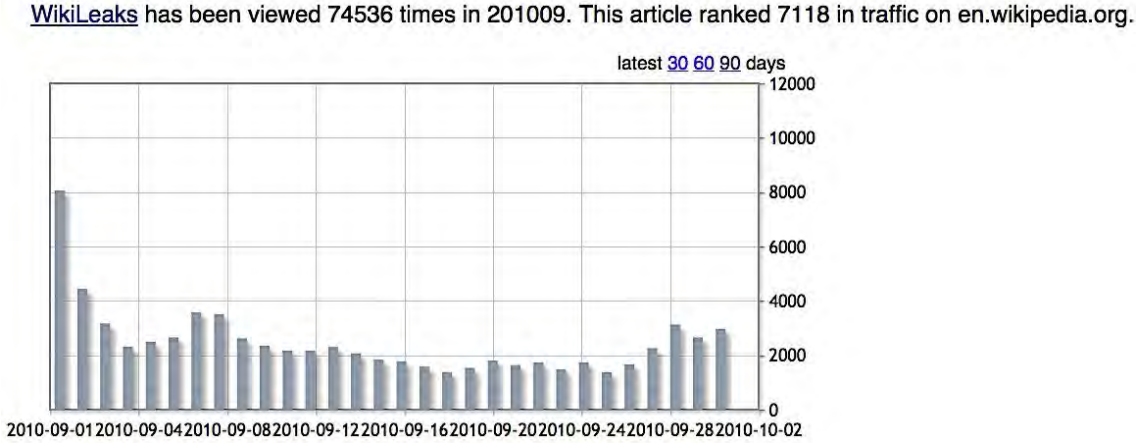
Gráfico 37: Evolución de visitas a la página de WikiLeaks en Wikipedia en octubre de 2010.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Las consultas al *wiki* caen estrepitosamente en septiembre de 2010, registrándose 74.536 sesiones, siendo el día 1 el de máxima actividad, con 8.059 visitas, cuando la Fiscalía sueca decidió reabrir el caso contra Assange por presunto acoso y violación.

Gráfico 38: Evolución de visitas a la página de WikiLeaks en Wikipedia en septiembre de 2010.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

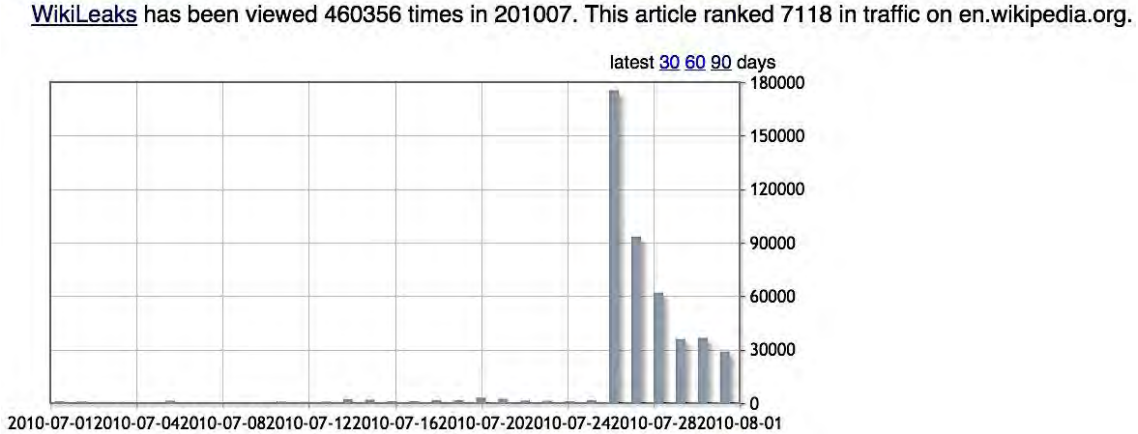
En agosto de 2010 se registraron 305.118 consultas, siendo el día 1 el de mayor actividad con 24.636 consultas, después de que WikiLeaks revelase los documentos secretos de la guerra en Afganistán y de que se anunciase la existencia del archivo encriptado *insurance.aes2560*.

Gráfico 39: Evolución de visitas a la página de WikiLeaks en Wikipedia en agosto de 2010.

Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

En julio, con la publicación de los documentos de la guerra en Afganistán, la página de WikiLeaks en Wikipedia fue visitada 460.356 veces, siendo el día 26 el de mayor actividad, con 175.431 consultas el mismo día que se dio a conocer esta filtración masiva.

Gráfico 40: Evolución de visitas a la página de WikiLeaks en Wikipedia en julio de 2010.

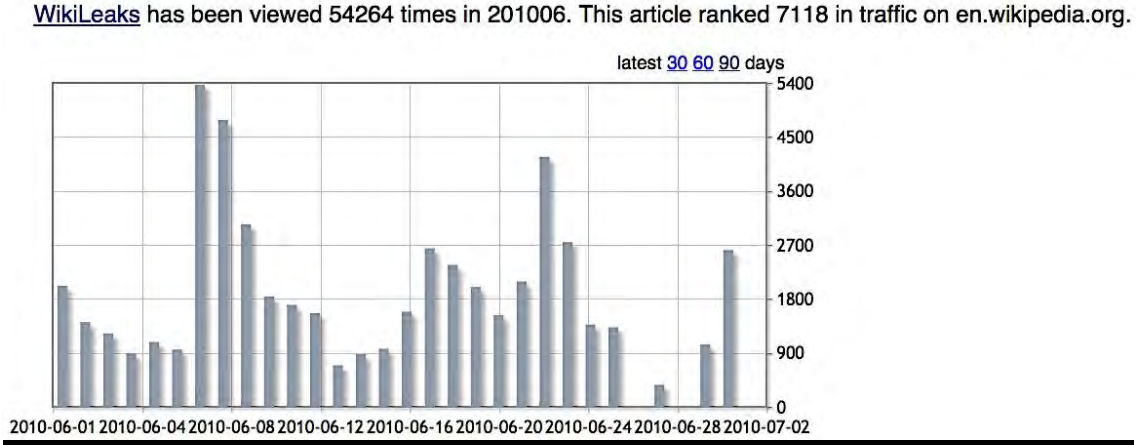


Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

En los siguientes gráficos podemos ver cómo el impacto de la página de WikiLeaks en Wikipedia fue mucho menor durante el primer semestre de 2010, antes de las filtraciones masivas de documentos. En junio, el número total de visitas fue de 54.264, con un pico máximo el día 7, con 5.369 consultas, cuando se supo que WikiLeaks estaba solicitando direcciones de correo electrónico militares —con el dominio *.mil*—, tras la detención del soldado Bradley Manning.

Ilustración 58: WikiLeaks [wikileaks]. (2010, May 07). We would like a list of as many .mil email addresses as possible. Please contact editor@wikileaks.org or submit [Tweet]. Recuperado de https://twitter.com/wikileaks/status/13570878440

Gráfico 41: Evolución de visitas a la página de WikiLeaks en Wikipedia en junio de 2010.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

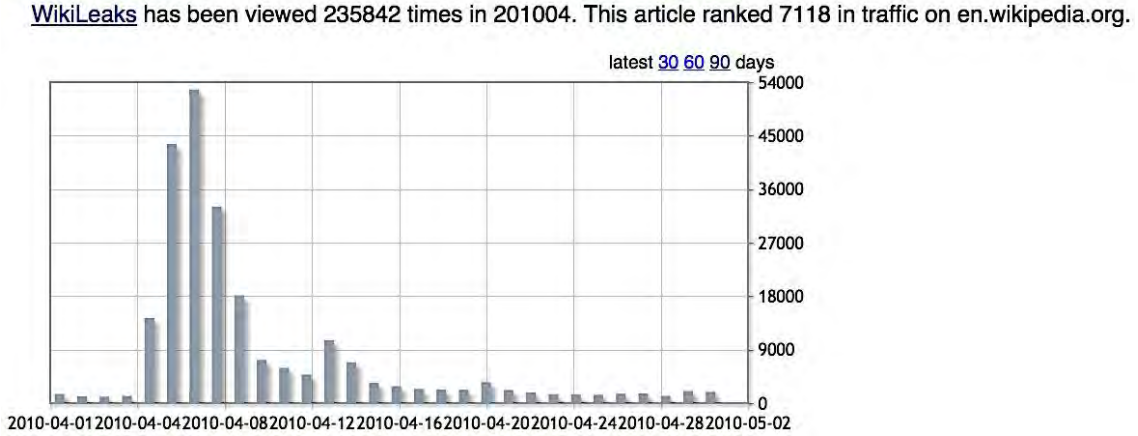
En mayo, se registraron 40.125 consultas, con un pico máximo de 4.358 el día 26, cuando Manning fue arrestado.

Gráfico 42: Evolución de visitas a la página de WikiLeaks en Wikipedia en mayo de 2010.

Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

En abril de 2010 se produjo la primera gran marea de visitas a la página de WikiLeaks en Wikipedia, coincidiendo con la primera filtración con impacto mundial: la revelación del vídeo *Collateral Murde*r, el día 5. Dos días después se registró el mayor volumen de tráfico en este *wiki* hasta ese momento, con 52.754 consultas.

Gráfico 43: Evolución de visitas a la página de WikiLeaks en Wikipedia en abril de 2010.



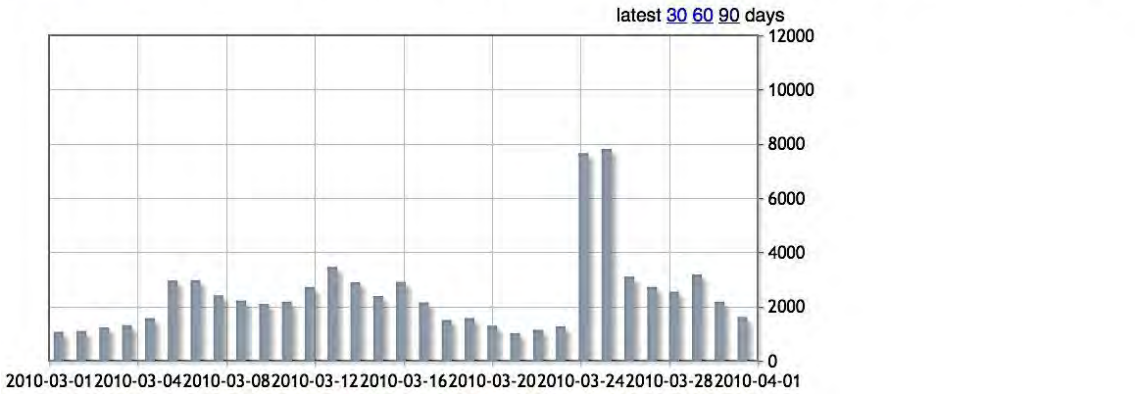
Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Antes de *Collateral Murder*, el *wiki* de WikiLeaks recibió 76.243 visitas en marzo de 2010, siendo el día 25 el de mayor tráfico, con 7.809 consultas, tras una alerta publicada por WikiLeaks en su cuenta en Twitter para denunciar que sus miembros estaban siendo vigilados por agentes de los servicios de inteligencia de Estados Unidos mientras trabajaban en los preparativos de la publicación del vídeo *Collateral Murder*.

Ilustración 59: WikiLeaks [wikileaks]. (2010, Mar 24). WikiLeaks is currently under an aggressive US and Icelandic surveillance operation. Following/photographing/filming/detaining. [Tweet]. Recuperado de https://twitter.com/wikileaks/status/10961072669

Unos días antes, el 15 de marzo, WikiLeaks había publicado un informe de treinta y dos páginas del Centro de Contrainteligencia del Ejercito de Estados Unidos, fechado el 18 de marzo de 2008 y titulado *Wikileaks.org - An Online Reference to Foreign Intelligence Services, Insurgents, Or Terrorist Groups?*. En este documento se detallaban numerosos métodos para destruir o marginar a WikiLeaks, principalemente mediante la persecución política a sus miembros. Tras la denuncia de WikiLeaks en Twitter, las visitas a su *wiki* en Wikipedia se dispararon los días 24 y 25 de marzo.

Gráfico 44: Evolución de visitas a la página de WikiLeaks en Wikipedia en marzo de 2010.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

En febrero de 2010, la página de WikiLeaks en Wikipedia recibió 63.100 visitas, registrándose el pico más alto el día 25, con 6.235 consultas, y cifras similares el 24. En ese periodo, WikiLeaks publicó el primer documento que Bradley Manning

había enviado a la organización, un cable sobre el escándalo financiero de Icesave, filial del banco islandés Landsbankin, cuya quiebra, en octubre de 2008, afectó a unos 350.000 ahorradores británicos y holandeses. El 14 de febrero de 2010, Manning envió a WikiLeaks un cable diplomático de Estados Unidos de dos páginas, fechado el 13 de febrero, titulado *Reykjavik-13*, en el que se hace referencia directa al caso de Icesave. WikiLeaks hizo público este cable el 18 de febrero. Al mismo tiempo, Assange y su equipo estaban trabajando ya en el vídeo de *Collateral Murder*, enviado también en febrero por Manning. El 21 de ese mes, la organización anunció que había logrado desencriptar un vídeo del Ejército de Estados Unidos en el que se veía cómo periodistas y civiles eran ametrallados.

Ilustración 60: WikiLeaks [wikileaks]. (2010, Feb. 21). Finally cracked the encryption to US military video in which journalists, among others, are shot. Thanks to all who donated $/CPUs. [Tweet]. Recuperado de https://twitter.com/wikileaks/status/9412020034

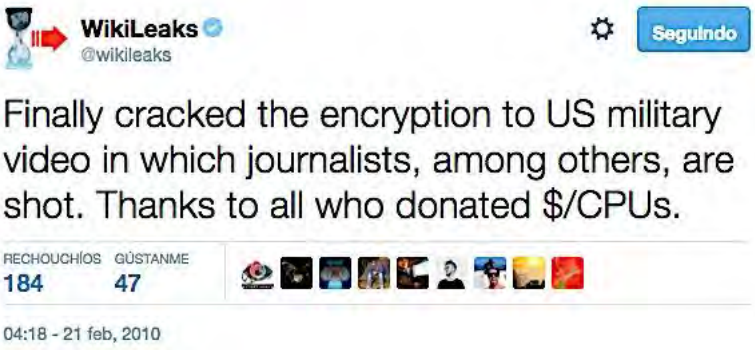
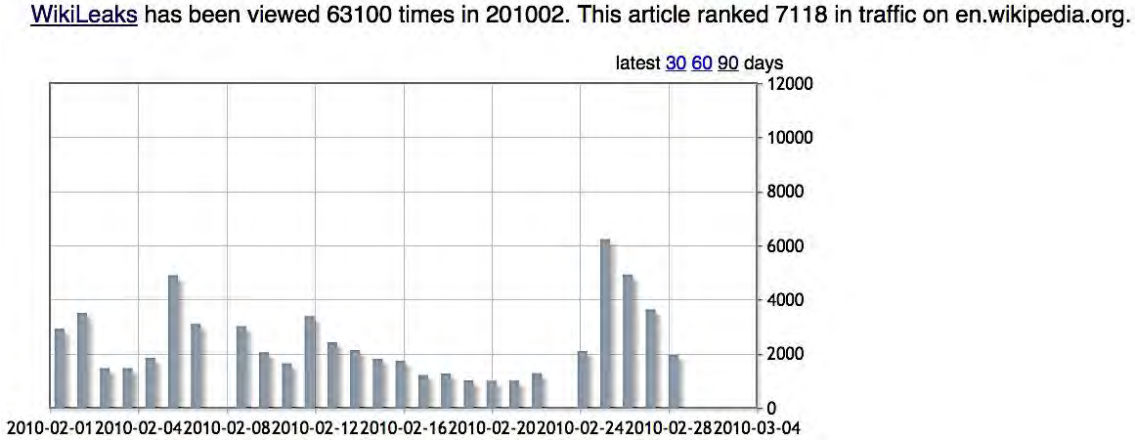


Gráfico 45: Evolución de visitas a la página de WikiLeaks en Wikipedia en febrero de 2010.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

En enero de 2010, la página de WikiLeaks en Wikipedia recibió 64.438 visitas, concentrándose el mayor volumen el día 28, con 7.147 consultas. Durante ese mes, WikiLeaks había empezado a colaborar en la Icelandic Modern Media Initiative, que posteriormente dio lugar al International Modern Media Institute, que ha convertido a Islandia en un paraíso seguro para informadores y filtradores. En esos días también se conoció que WikiLeaks había suspendido temporalmente sus actividades relacionadas con las filtraciones de documentos secretos por falta de fondos económicos para mantener su infraestructura.

Gráfico 46: Evolución de visitas a la página de WikiLeaks en Wikipedia en enero de 2010.

Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Para acabar de completar nuestro análisis, mostramos los datos de tráfico en Wikipedia en otros dos momentos cruciales para nuestra investigación: el desencuentro público entre WikiLeaks y los cinco medios que colaboraron inicialmente en el *Cablegate*, y las revelaciones de los correos electrónicos de Stratfor, la filtración más impactante, por su volumen, tras las publicaciones del año 2010. De nuevo, comprobamos que no se alcanzó el nivel de impacto conseguido durante el *Cablegate*.

El 1 de septiembre de 2011, WikiLeaks y los medios con los que había colaborado en el *Cablegate* escenificaron sus desencuentros con sendas publicaciones editoriales criticándose los unos a los otros por la liberación en bruto de la totalidad de los cables de Estados Unidos. Ese mes, el *wiki* de WikiLeaks rozó las 225.000 visitas, siendo el día 6 el de mayor tráfico con 25.325 consultas, en plena disputa dialéctica entre las partes.

Gráfico 47: Evolución de visitas a la página de WikiLeaks en Wikipedia en septiembre de 2011.

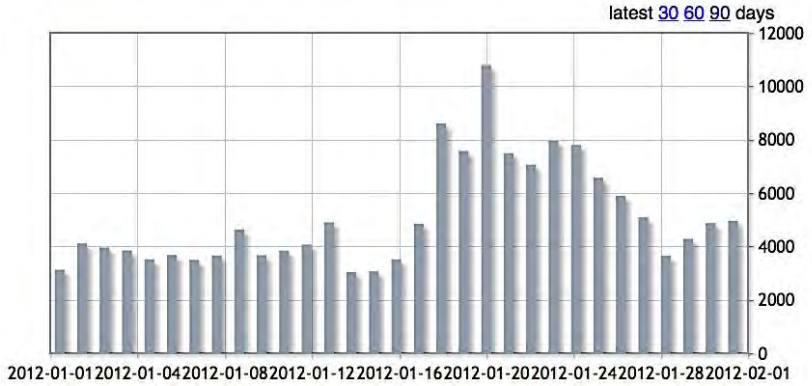
Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Por último, WikiLeaks anunció el 27 de febrero de 2012 la mayor filtración de documentos secretos de la historia: cinco millones y medio de correos electrónicos de la agencia de inteligencia global Stratfor. Sin embargo, como hemos visto también en las estadísticas de búsquedas en Google, en el impacto en redes sociales y en la evolución del tráfico estimado de la página web de WikiLeaks, y pese a involucrar a más medios en estas filtraciones, las visistas a la página de WikiLeaks en Wikipedia estuvieron muy por debajo del nivel alcanzado durante el *Cablegate*, por lo que concluimos que el interés generado y la influencia de WikiLeaks en la opinión pública decayeron notablemente.

Como pudimos corroborar con los datos de los siguientes gráficos, la mayor filtración de documentos secretos de la historia, por su volumen, no despertó mayor atención sobre WikiLeaks, ni siquiera un interés similar. En enero de 2012, su *wiki* fue consultado 157.611 veces; en febrero cayó a 134.393 visitas, de las cuales 11.185 (8,3 por ciento) se registraron el día 27, el pico más alto ese mes, coincidiendo con el anuncio de estas filtraciones. La tendencia negativa continuó en marzo, con 109.406 consultas, con un máximo de 5.963 el día 7.

Gráfico 48: Evolución de visitas a la página de WikiLeaks en Wikipedia en enero de 2012.

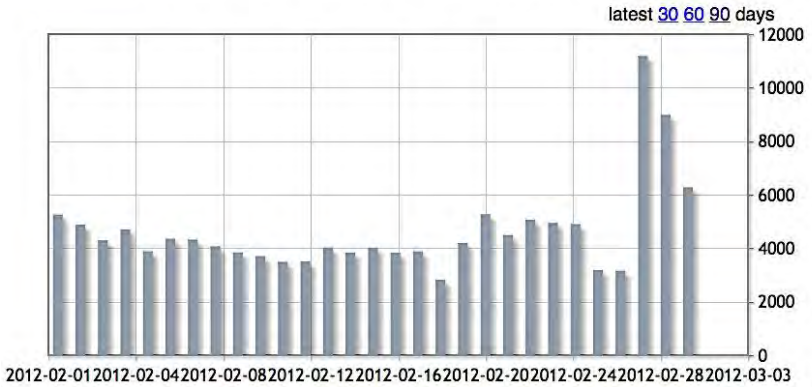
WikiLeaks has been viewed 157611 times in 201201. This article ranked 7118 in traffic on en.wikipedia.org.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Gráfico 49: Evolución de visitas a la página de WikiLeaks en Wikipedia en febrero de 2012.

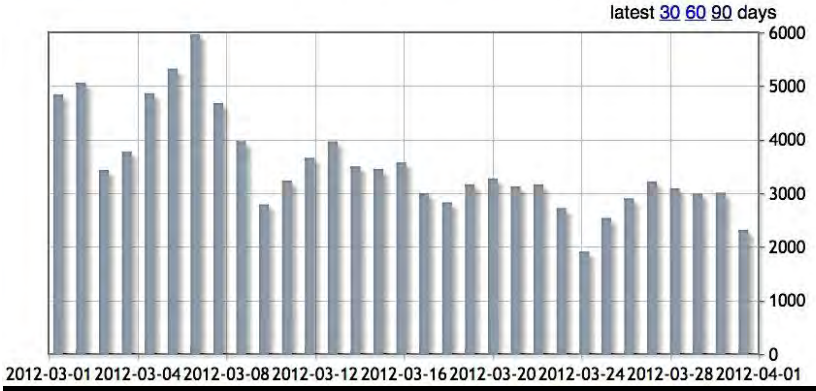
WikiLeaks has been viewed 134393 times in 201202. This article ranked 7118 in traffic on en.wikipedia.org.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

Gráfico 50: Evolución de visitas a la página de WikiLeaks en Wikipedia en marzo de 2012.

WikiLeaks has been viewed 109406 times in 201203. This article ranked 7118 in traffic on en.wikipedia.org.



Fuente: captura de pantalla propia tomada de Stats.Grok.se (acceso: 16 de octubre de 2015).

IV.10. WIKILEAKS EN LAS PORTADAS DE *THE NEW YORK TIMES*, *THE GUARDIAN*, *LE MONDE* Y *EL PAÍS*

Tras constatar que el *Cablegate* marcó el cenit de WikiLeaks, seleccionamos todas las cabeceras implicadas en este caso, excepto *Der Spiegel* —excluida por su frecuencia semanal—, para observar la evolución diaria de las publicaciones sobre WikiLeaks en el periodo de tiempo de máximo impacto, entre el 29 de noviembre y el 31 de diciembre de 2010. Para ello utilizamos el software libre de código abierto PageoneX, ideado por el arquitecto español Pablo Rey-Mazón para la codificación, análisis y visualización de informaciones en las portadas en papel de periódicos de todo el mundo[197].

Una vez obtenidas en orden cronológico todas las portadas de *The New York Times*, *The Guardian*, *Le Monde* y *El País* del periodo seleccionado, iniciamos un proceso de codificación portada a portada para la visualización del espacio ocupado por el universo WikiLeaks en las páginas principales de estos periódicos.

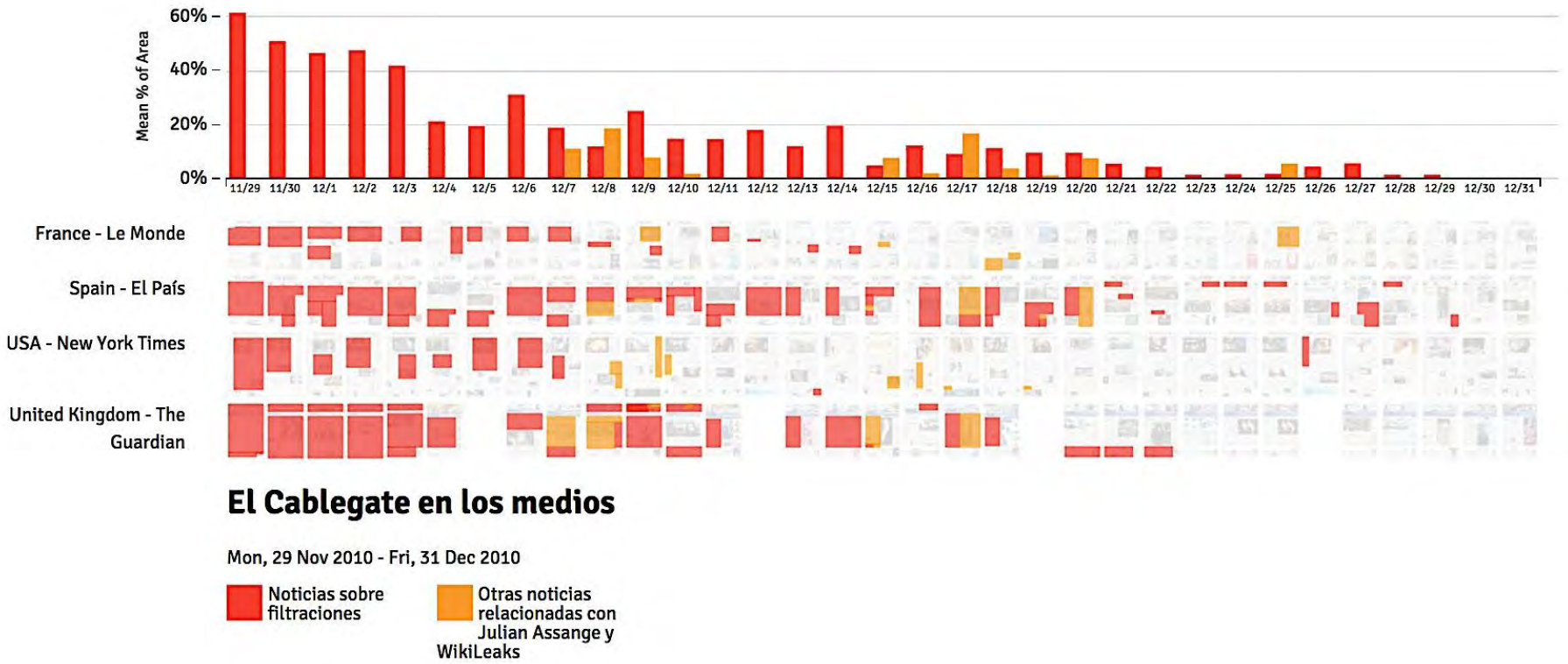
Para nuestra visualización decidimos codificar por colores las áreas ocupadas por el universo WikiLeaks en dos categorías:

1) En rojo, noticias sobre las filtraciones de los cables diplomáticos de Estados Unidos.
2) En naranja, otras noticias relacionadas con WikiLeaks y Julian Assange.

Los espacios no codificados corresponden a áreas no ocupadas por informaciones relativas o vinculadas a WikiLeaks, es decir, otras noticias, espacios publicitarios y cabeceras de los periódicos. Por último, dado que la edición en papel del periódico británico *The Guardian* se publica de lunes a sábado, los días 5, 12, 19 y 26 de diciembre —todos en domingo— quedan en blanco en la visualización de datos.

[197] Véase apartado 5.2.5. de la Introducción.

Gráfico 51: Espacio dedicado a WikiLeaks en las portadas de *Le Monde*, *El País*, *The New York Times* y *The Guardian*.



Fuente: elaboración propia usando PageOneX. Disponible en: http://pageonex.com/Alberto_Quian/impacto-de-wikileaks-en-los-medios/.

Gráfico 52: Espacio dedicado a los cables diplomáticos en las portadas de *Le Monde*, *El País*, *The New York Times* y *The Guardian*.

Fuente: elaboración propia usando PageOneX. Disponible en: http://pageonex.com/Alberto_Quian/impacto-de-wikileaks-en-los-medios/.

Gráfico 53: Espacio dedicado a otras informaciones sobre WikiLeaks en las portadas de *Le Monde*, *El País*, *The New York Times* y *The Guardian*.

Fuente: elaboración propia usando PageOneX. Disponible en: http://pageonex.com/Alberto_Quian/impacto-de-wikileaks-en-los-medios/.

En esta visualización comprobamos que, con gran diferencia, el 29 de noviembre de 2010 es el día que mayor impacto tuvo el *Cablegate* en las portada en papel de los medios colaboradores de WikiLeaks, coincidiendo con el anuncio de las filtraciones. Ese día, en conjunto, el *Cablegate* ocupó el 61 por ciento del espacio total de las portadas de los medios analizados, liderados por *The Guardian* y *The New York Times*, que dedicaron la casi totalidad de sus portadas a este caso, seguidos por *El País* y, en menor medida, *Le Monde*, lo cual nos indica el papel crucial que jugaron el periódico británico y el estadounidense como actores principales.

En los días inmediatamente posteriores, entre el 30 de noviembre y el 3 de diciembre, las filtraciones de los cables diplomáticos ocuparon entre el 50.4 por ciento y el 41,4 por ciento del espacio total de las portadas de estos periódicos, monopolizando la primera página de *The Guardian*. En *The New York Times* vemos que siguió siendo el tema central, aunque disminuyó su peso una vez anunciada la publicación de los cables. En *El País* también fue el tema central durante esos primeros días, ocupando casi toda la portada. *Le Monde* fue, desde el inicio, el periódico que menos importancia dio al *Cablegate* en su primera página.

El interés de estos periódicos en las filtraciones de los cables diplomáticos cayó de forma abrupta a partir del sexto día, constatándose una progresiva disminución de las noticias sobre las filtraciones, hasta su desaparición a finales de diciembre de 2010. El 4 de diciembre, el *Cablegate* ya sólo ocupaba el 20,8 por ciento de la superficie total de las cuatro portadas, y el día 5, el l9,1 por ciento. El día 6 hubo un pequeño repunte, hasta el 30,6 por ciento.

Los días 7 y 8 de diciembre se produjo un punto de inflexión: los cables empezaron a pasar a un segundo plano y ganaron espacio otras noticias relacionadas con el caso judicial de Assange, el bloqueo al que fue sometida la organización y las acciones del grupo hacktivista Anonymous en apoyo a WikiLeaks. Durante esos dos días, el universo WikiLeaks dominó casi un tercio del espacio de las portadas de estas cabeceras.

El 7 de diciembre, *The Guardian* empezó a centrar la atención sobre los problemas que Assange enfrentaba con la justicia, asunto que ocupó casi toda su primera página. Ese día, en el conjunto de los periódicos analizados, los cables apenas llenaron un 18,4 por ciento de la superficie de las portadas, mientras que, gracias a *The Guardian*, Assange ocupó el 10,6 por ciento.

El día 8 se confirma un cambio de tendencia en las portadas, cuando todos, excepto *Le Monde* —que lo haría un día después—, dedicaron espacios destacados a la detención del fundador de WikiLeaks. Ese día, el periódico francés dedicó un pequeño espacio en su portada a información extraída de los cables; *El País* repartió más de la mitad de su portada entre la detención de Assange e información obtenida de los documentos filtrados; *The New York Times* sólo se centró en la detención del fundador de WikiLeaks en un espacio reducido, y *The Guardian*, de nuevo, volvió a dedicar casi la totalidad de su primera página a WikiLeaks, con la detención de Assange como tema principal. Las noticias dedicadas a las filtraciones sólo ocuparon el 11,5 por ciento de las portadas del 8 de diciembre, mientras que las informaciones sobre Assange llenaron el 18,1 por ciento del espacio total.

El 9 de diciembre, a los cables y el caso judicial de Assange se sumaron los primeros ciberataques contra los sitios que participaron en el bloqueo a WikiLeaks. *Le Monde* informó sobre la detención de Assange; *The New York Times*, sólo sobre las acciones de los hackers en defensa del fundador de WikiLeaks; por su parte, *El País* y *The Guardian* dieron prioridad a los contenidos de los cables, pero introdujeron breves referencias a la denomianda *Operation Avenge Assange*, transmutación de la campaña hacktivista *Operation Payback*. Gracias al interés que aún mantuvieron en destacar los cables el periódico británico y, en menor medida, el español, el fenómeno WikiLeaks siguió ocupando casi un tercio de la superficie del conjunto de las portadas: un 24,6 por ciento para los cables y un 7,4 por ciento para informaciones sobre la detención de Assange y las acciones de los hackers en la Red.

De ahí en adelante, *The New York Times* y *Le Monde* fueron perdiendo de manera notable el interés en WikiLeaks y sólo *The Guardian* y *El País* mantuvieron la tensión informativa, hasta que a finales de diciembre el fenómeno WikiLeaks se evaporó.

Entre los días 10 y 20 de diciembre, el espacio dedicado en las portadas de estos periódicos a informaciones relacionadas con WikiLeaks fluctuó entre el 19,1 (el día 14) y el 10 por ciento (el día 20), excepto el día 17, cuando se produjo un pequeño repunte hasta el 24,8 por ciento gracias a los grandes espacios que *The Guardian* y *El País* dedicaron a la liberación de Assange y, en menor medida, a los cables. Ese día, *The New York Times* minimizó en su primera página la noticia de la salida del fundador de WikiLeaks. Por su parte, *Le Monde* informó sobre la liberación de Assange un día

después. En total, el espacio dedicado a Assange en las cuatro portadas del día 17 fue el 16,4 por ciento y el reservado a los cables, el 8,6 por ciento.

Desde el 21 de diciembre, las informaciones sobre cualquier tema vinculado a WikiLeaks ocuparon un espacio máximo del 6,3 por ciento (día 25) y un mínimo del 0,9 por ciento (día 23), antes de desaparecer por completo los días 30 y 31. En este periodo prácticamente ya sólo *El País* siguió publicando en portada noticias basadas en los cables diplomáticos; *The Guardian*, que hasta entonces había dedicado los mayores espacios a las filtraciones, ya no mostró interés en destacarlas en su primera página; por su parte, *The New York Times* solamente publicó dos informaciones relacionadas con el *Cablegate* entre los días 8 y 31 de diciembre, una de un debate en la Red sobre la liberación de los documentos (día 13) y otra sobre la guerra contra el narcotráfico recogida de los cables diplomáticos (día 26); por último, *Le Monde*, cuyas publicaciones en portada sobre WikiLeaks fueron ínfimas desde el día 12, disparó la atención sobre Assange el día 25, al ser elegido "hombre del año" por la propia redacción del periódico francés.

IV.11. ANÁLISIS TEXTUAL DE LA CRISIS ENTRE WIKILEAKS Y SUS CINCO SOCIOS EN EL *CABLEGATE*

Mostramos a continuación los resultados de nuestro análisis de los textos publicados por WikiLeaks y sus socios en el *Cablegate* en plena crisis entre ambas partes. Estos datos se obtuvieron usando la versión beta de Linguakit[198], por lo que podrían variar en otros análisis con el mismo software mejorado o con otro similar. Ofrecemos datos comparativos extraídos del editorial de WikiLeaks del 1 de septiembre de 2011 —en el que se justificó la liberación de todos los cables diplomáticos en bruto— y de la respuesta crítica de sus colaboradores, encabezados por *The Guardian* con un artículo del 2 de septiembre de 2011 que incluye la declaración conjunta de las cinco cabeceras.

Tabla 6: Análisis estadístico de los textos de WikiLeaks y *The Guardian*.

Variables	WikiLeaks 'Guardian journalist negligently disclosed Cablegate passwords'	The Guardian 'WikiLeaks publishes full cache of unredacted cables'
Caracteres (sin espacios)	8.234	4.408
Palabras	1.717	881
Sustantivos	184	117
Verbos	136	72
Adjetivos	70	41
Adverbios	49	28
Lemas diferentes	605	348
Frases	66	33
Variedad léxica	57,27%	58,58%
Sentimiento del texto	Negativo	Negativo
Grado de sentimiento negativo	2,35%	10,5%
Frases positivas	25	10
Frases neutras	16	8
Frases negativas	25	15
Palabra clave	*WikiLeaks*	*WikiLeaks*
Sustantivo común más usado	*cable*	*cable*
Frecuencia del sustantivo más usado	16	9
Adjetivo más usado	*unpublished* y *human*	*new* y *former*
Frecuencia del adjetivo más usado	4	4
Entidad más relevante	WikiLeaks	WikiLeaks
Frecuencia de la entidad más relevante	28	18
Multipalabra con más peso	*human rights*	*full archive*
Peso de la multipalabra	27,75	5,89

Fuente: elaboración propia a partir de los datos obtenidos con Linguakit.

[198] Véase apartado 5.2.4. de la Introducción.

Lo primero que observamos es que la extensión del editorial de WikiLeaks prácticamente dobla a la del artículo del periódico británico, lo cual denota una necesidad mayor en WikiLeaks que en *The Guardian* de proporcionar más información y de dar más explicaciones para justificarse ante la opinión pública.

En cuanto a la calidad de los textos, vemos que la variedad léxica es prácticamente la misma en términos porcentuales. Si observamos la densidad de sustantivos, verbos, adverbios y adjetivos únicos utilizados, comprobamos que los porcentajes son muy parecidos, excepto en el caso de los nombres. Así, el porcentaje de sustantivos únicos sobre el total de palabras en el texto de WikiLeaks es del 10,71 por ciento, mientras que en el artículo de *The Guardian* es del 13,28; en el caso de los verbos es del 7,92 por ciento y del 8,17, respectivamente; para los adjetivos, el 4,07 por ciento y el 4,65, y los adverbios, el 2,85 por ciento y el 3,17. Por lo tanto, desde un punto de vista formal, los textos de WikiLeaks y *The Guardian* son similares, si bien en el artículo del periódico vemos que hay mayor variedad de sustantivos que le dan un poco más de variedad léxica.

En ambos textos vemos que domina un sentimiento negativo, pero es más acusado en el artículo de *The Guardian*, donde las frases valoradas como negativas superan a las positivas y neutras, mientras que el de WikiLeaks está próximo a una neutralidad, *a ojos* de los algoritmos.

También constatamos coincidencias en la palabra clave y entidad más relevantes, *WikiLeaks*, y en el sustantivo común más usado, *cable*.

A continuación mostramos tres tablas en las que comparamos las entidades, sustantivos y adjetivos más frecuentes en ambos textos. Esto nos ayuda a comprender qué conceptos y temas son los más sustanciales para WikiLeaks y *The Guardian* para armar sus discursos, y nos permite identificar semejanzas y diferencias entre ambos artículos.[199]

[199] Limpiamos los datos eliminando resultados inválidos, en concreto: la identificación del número '1' como segunda entidad más frecuente en WikiLeaks, 's' como sexto sustantivo más repetido también en WikiLeaks, y '1' y '5' como primera y sexta entidades en *The Guardian*. Dado que el software estaba en fase beta, vimos otras funcionalidades mejorables, como la asignación de etiquetas en el Reconocedor de Entidades. Por ejemplo, encontramos que a la entidad 'WikiLeaks' se le asignaban las etiquetas 'organización', 'persona, 'localidad' y 'miscelánea', o que 'Assange' era etiquetado como 'organización'. En todo caso, esto no afectó sustancialmente a nuestros resultados y puede ser corregido por el investigador en un proceso de limpieza de datos, aprobando, rechazando o corrigiendo manualmente los datos obtenidos.

Tabla 7: Entidades más frecuentes en los textos de WikiLeaks y *The Guardian*.

WikiLeaks		*The Guardian*	
Frecuencia	**Lema**	**Frecuencia**	**Lema**
28	wikileaks	18	wikileaks
17	guardian	7	which
12	leigh	6	assange
6	assange	5	guardian
6	US	2	who
5	david_leigh	2	12/2010
5	that	2	US
5	what	2	julian_assange
4	state_department	1	twitter
4	who	1	daniel_domscheit

Fuente: elaboración propia a partir de los datos obtenidos con Linguakit.

Tabla 8: Sustantivos comunes más usados en los textos de WikiLeaks y *The Guardian*.

WikiLeaks		*The Guardian*	
Frecuencia	**Lema**	**Frecuencia**	**Lema**
16	cable	9	cable
8	book	7	file
8	password	7	password
7	publication	5	site
5	right	5	document
5	security	4	source
4	journalist	4	organisation
4	time	3	danger
4	week	3	government
4	year	3	archive

Fuente: elaboración propia a partir de los datos obtenidos con Linguakit.

Tabla 9: Adjetivos más usados en los textos de WikiLeaks y *The Guardian*.

WikiLeaks		*The Guardian*	
Frecuencia	**Lema**	**Frecuencia**	**Lema**
4	unpublished	4	new
4	human	4	former
3	unredacted	3	full
3	political	3	previous
3	complete	3	temporary
3	last	2	sensitive
3	diplomatic	2	joint
3	past	2	available
3	other	2	technical
2	safe	1	diplomatic

Fuente: elaboración propia a partir de los datos obtenidos con Linguakit.

Las entidades nos dicen principalmente quién está implicado en la disputa. Así, vemos que se articula una discusión con cuatro actores principales: dos organizaciones enfrentadas, WikiLeaks y *The Guardian*, y su disputa personalizada en Julian Assange y el periodista David Leigh, autor del libro *WikiLeaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia* (2011). En esta tensión dialéctica emerge como actor secundario el Gobierno de Estados Unidos (entidades *US* y *state_department*), en dos discursos que intentan responder a las preguntas básicas sobre la relación entre las partes y los motivos de su ruptura: qué, quién, cuándo y cómo.

Los sustantivos comunes nos aclaran el tema principal de la discusión. Vemos que *cable* (en sus formas en singular y plural) y *password* son los sustantivos más frecuentes en los que coinciden WikiLeaks y *The Guardian*. Esto nos sugiere que para ambas partes es importante centrar sus discursos en la liberación de los cables diplomáticos de Estados Unidos y en la contraseña para desencriptarlos, origen de la discordia. De la lista de sustantivos más repetidos por WikiLeaks deducimos, además, que se afana en centrar la atención en el libro de Leigh (*book*) como el objeto dañino y en conceptos clave en el universo WikiLeaks como *publicación* (publication), *seguridad* (security), *derechos* (right) y *periodismo/periodistas* (*journalist*).

Observamos también lo importante que es para WikiLeaks contextualizar temporalmente los hechos (*time*, *year*, *week*). Frente al libro de Leigh como objeto de discusión y a las abstracciones referidas en el editorial de WikiLeaks, el texto de *The Guardian* fija la atención en lo tangible, esto es, archivos, ficheros, documentos, sitios web, fuentes de información (*file*, *site*, *document*, *source*, *archive*).

Nos parece sustancial destacar también el uso repetido que *The Guardian* hace de la palabra *organisation* para referirse a los medios colaboradores de WikiLeaks en el *Cablegate*; éstos ya no son empresas ni periódicos, sino organizaciones mediáticas, como WikiLeaks, aunque con sustanciales diferencias estructurales, organizativas, operativas, financieras, estratégicas y éticas.

Además, frente al concepto de seguridad (*security*) que se halla en el discurso WikiLeaks, *The Guardian* contrapone el de *peligro* (*danger*), con el que imprime un sentimiento negativo sobre WikiLeaks en un discurso alarmante. A la seguridad que reclama WikiLeaks para sí, el periódico británico contrapone las amenazas potenciales para las fuentes que aparecen en los cables diplomáticos sin editar.

Para finalizar, el uso recurrente de determinados adjetivos nos dice cómo WikiLeaks y *The Guardian* describen e interpretan a los actores y los temas que tratan. En el texto de WikiLeaks vemos un uso recurrente de adjetivos como *unpublished* y *unredacted* (*inédito* y *sin editar*) que parecen imprimir una gravedad periodística a un discurso en el que, además, hay una importante carga política (*political*, *diplomatic*) y de *humanidad* (*human*).

En el artículo de *The Guardian* es muy significativo el uso elocuente que se hace del adjetivo *former* para hablar de exsocios y excolaboradores de WikiLeaks e insistir en la idea de que esta organización es fuente de conflictos y de rupturas.

En ambos textos, adjetivos como *full* y *complete* (*completo*), *available* (*disponible*), *temporary* (*temporal*), *safe* (*seguro*) o *sensitive* (*sensible*) se repiten alrededor del tema central, los cables, mientras que el uso de adjetivos como *previous* (*previo*), *last* (*último*) o *past* (*pasado*) nos sitúan en los antecedentes de la controversia.

Para completar este análisis, mostramos en una *nube* los términos multipalabra más relevantes, siendo los de mayor tamaño los de mayor peso en los artículos de WikiLeaks y *The Guardian*. Estas nubes nos sirven como resúmenes abstractos de los textos, de manera que podemos visualizar en una imagen el contenido básico de los artículos y ver cuál es su *leitmotiv*. El extractor multipalabra amplía la búsqueda del extractor de palabras, de manera que obtenemos los grupos de palabras más importantes de cada texto y tenemos una mejor selección del léxico más relevante del texto.

Con el extractor multipalabra constatamos que para WikiLeaks la defensa de los derechos humanos (*human rights*) es un asunto central, sobre el que gira la polémica sobre la liberación de todos los cables diplomáticos de Estados Unidos, mientras que para *The Guardian* lo es el propio archivo completo que contiene los cables (*full archive*). Pero el peso de la multipalabra central en el artículo de WikiLeaks (27,75) es mucho mayor que la del texto del periódico británico (5,89), como hemos visto en la Tabla 6. Vemos, además, que hay un mayor equilibrio entre las multipalabras más importantes de *The Guardian* que en las de WikiLeaks.

Ilustración 61: : Nube de multipalabras para el texto de WikiLeaks.

Fuente: elaboración propia con Linguakit.

Ilustración 62: Nube de multipalabras para el texto de *The Guardian*.

Fuente: elaboración propia con Linguakit.

CONCLUSIONES

Primera

El progreso de la computación, el desarrollo y democratización de nuevas tecnologías digitales de la información y la comunicación, y la expansión de la Red son decisivos en el florecimiento de la ética y la cultura hackers —en las que hunde sus raíces WikiLeaks— como espíritu alternativo para la sociedad red, y son fundamentales para la manifestación de la dimensión política del *hacking*. De nuestro análisis de la ética y la cultura hackers y de nuestro caso de estudio concluimos que WikiLeaks es un nuevo eslabón en el proceso evolutivo hacker, determinado por el desarrollo de la sociedad red y, fundamentalmente, por la democratización de la Red con la irrupción de Internet y de las comunidades virtuales y redes sociales en línea, en las que los hackers fueron pioneros. WikiLeaks marca un nuevo estadio evolutivo hacker que recoge como aprendizaje todas las experiencias, progresos y fracasos anteriores de los hackers implicados en el desarrollo de una auténtica sociedad del conocimiento.

En el fenómeno WikiLeaks encontramos la curiosidad, el espíritu juguetón y la libertad que caracterizó a los primeros hackers; la pasión por la alta tecnología, la actitud antiautoritaria y el deseo de abrir lo hermético y de compartir hazañas y conocimientos que fueron desarrollando las primeras comunidades hackers; el anhelo de emancipación que empezaron a mostrar en la década de 1980 las primeras organizaciones hackers y su defensa de la libertad de información; la protección de la privacidad y de una Internet libre que exigieron *cypherpunks* y ciberlibertarios a principios de la década de 1990, y la defensa activa de los derechos humanos que emprendieron los primeros hacktivistas en la segunda mitad de la misma década, con la libertad de expresión como derecho fundamental a proteger. WikiLeaks y Assange son herederos naturales de los primeros hackers del Massachusetts Institute of Technology; de Kevin Mitnick, Edward Cummings, Mark Abene y Craig Neidorf; de Cult of the Dead Cow y del Chaos Computer Club; de *2600*, *Phrack*, Cryptome.org y la lista *Cypherpunks*; de la Free Software Foundation y la Electronic Frontier Foundation, o del proyecto Hacktivismo. Y se hermana y complementa con Anonymous, la mayor red hacktivista articulada para la desobediencia civil híbrida.

Los principios y esencias de los primeros héroes de la cultura hacker, de los primeros medios y las primeras comunidades hackers, de las primeras organizaciones ciberlibertarias y hacktivistas, y de la red transnacional Anonymous convergen y son mejorados en WikiLeaks como fenómeno hacktivista transversal e informacional.

Segunda

De nuestro análisis del fenómeno WikiLeaks y de nuestra observación participante inferimos que WikiLeaks propone en el campo de los medios de comunicación un nuevo modelo de organización en red y transnacional que modifica radicalmente los procesos de producción, gestión y difusión de la información, articulando una red de fuentes protegidas por la alta tecnología y enlaces seguros con las comunidades periodística, científica y activista para que los datos y la información fluyan libremente y se transformen en conocimiento y acción. WikiLeaks actúa como el nodo principal, facilitando las conexiones seguras de los demás nodos de esta red colaborativa, de manera que periodistas, científicos y activistas de todo el mundo pueden acceder, mediante enlaces con el nodo principal, a la información y a los datos proporcionados por fuentes protegidas. WikiLeaks se erige así en un agente que busca garantizar el flujo libre de información y promover procesos de producción de información autónomos, sin mediación ni injerencias del poder autoritario, articulando un sistema de redes informativas en las que subyacen valores de la ética hacker y que, en el caso del periodismo, nos lleva hacia una nueva ética periodística hacker.

Curiosidad, pasión, libertad, emancipación, autonomía, voluntariedad, antiautoritarismo, colaboración, verdad, transparencia, libre acceso a la información y al conocimiento, universalidad, preocupación responsable, valor y compromiso social, y confianza en la alta tecnología para mejorar la democracia y proteger los derechos humanos son los principios que se proponen para un nuevo periodismo más próximo al activismo informativo y que se opone a los procesos de mercantilización de la información, a la privatización del acceso a ésta, a las restriccciones del *copyright*, al modelo fordista y competitivo asimilado en las empresas informativas, a sus rutinas programadas para la producción en serie y publicación masiva de noticias blandas y de torrentes de opinión, a las injerencias de los poderes político y corporativo en todo el proceso de producción de la información y, en definitiva, a un modelo de periodismo

industrializado, mercantilizado, jerarquizado, comprometido por la cuenta de resultados y sometido al afán del beneficio económico.

WikiLeaks recupera, actualiza y vigoriza en los tiempos virales la tradición del periodismo *muckraker* que hace un siglo abrió en Estados Unidos, con sus *rastrillos*, el camino al periodismo de investigación y de denuncia; un periodismo que desconfía siempre del poder político y corporativo y de sus fuentes, que revuelve en su *basura* y que busca provocar reacciones. El periodismo *muckraker* ahora es hacker y dispone de alta tecnología digital y de redes de comunicación seguras para seguir removiendo la *basura* del poder.

Consideramos que aún es pronto para concluir si este nuevo modelo de periodismo en red, colaborativo, transnacional y hacker se consolidará, o si sucumbirá por la fuerza de los poderes corporativos-gubernamentales y del espíritu del capitalismo. En todo caso, de nuestra investigación y de la experiencia obtenida de nuestra participación en el proceso de producción informativa y publicación de los *GI Files* concluimos que la ética hacker, como desafío al espíritu dominate de la sociedad red, debe servir como marco también para una nueva ética periodística que devuelva a los periodistas la pasión, la creatividad y la libertad para trabajar, que combata la censura y extirpe la autocensura, que fomente la cooperación y que motive un compromiso firme e innegociable con la transparencia, el derecho a la privacidad, la libre expresión, la libre información, el acceso universal a los recursos para el conocimiento y su uso libre, la defensa de los derechos humanos y la promoción de la justicia social y del bien común.

Tercera

La historia de WikiLeaks se divide en tres etapas estratégicas claves, delimitadas por el distinto impacto alcanzado por sus filtraciones. La primera etapa se desarrolló desde finales de 2006 —cuando comenzó su actividad— hasta el 5 de abril de 2010. Durante este periodo, de plena autonomía editorial, WikiLeaks publicó numerosos documentos secretos de gran valor, sin embargo, su impacto mediático fue muy discreto, como hemos podido corroborar en esta investigación.

El primer punto de inflexión se produjo el 5 de abril de 2010, cuando WikiLeaks reveló el vídeo *Collateral Murder*, con el que se inició la segunda etapa. Por entonces,

Julian Assange ya había comprendido que necesitaba establecer relaciones más estrechas con los medios tradicionales, a los que siempre ha considerado correas de transmisión del poder político y corporativo. Para alcanzar el máximo impacto en la esfera pública debía valerse de sus *enemigos* naturales, por lo que decidió entablar colaboraciones directas con algunos de los principales y más influyentes medios de Occidente. Este cambio de estrategia coincidió con un hecho fundamental: WikiLeaks estaba recibiendo a principios de 2010 el mayor alijo de documentos secretos jamás filtrados, cientos de miles enviados a la organización por el soldado Manning, sobre las guerras de Irak y Afganistán, y sobre la diplomacia estadounidense. Y ni WikiLeaks ni ninguna organización informativa, por amplia que fuese, podía por sí sola gestionar un archivo tan vasto como el que había recibido. Así que se juntaron dos necesidades: una, la de aprovecharse de algunos de los medios más influyentes del mundo occidental para lograr el máximo impacto mediático y político, y en segundo lugar, la de contar con un equipo de colaboradores amplio y profesional que pudiese gestionar y editar una cantidad ingente de material en bruto, para pasarlo por el filtro periodístico y hacerlo digerible para el gran público. Así fue como WikiLeaks planeó las grandes filtraciones del año 2010, cuando alcanzó su cenit, en términos de impacto mediático y político; primero, con el vídeo *Collateral Murder*, que marca el primer punto de inflexión en la historia de WikiLeaks, al darse a conocer mundialmente, y luego, con las filtraciones masivas que se sucedieron durante aquel año: los *Papeles de la Guerra de Afganistán*, en julio de 2010, los *Diarios de la Guerra de Irak*, en octubre, y finalmente, el *Cablegate*, a finales de noviembre, con el que alcanzó su máximo impacto, como hemos comprobado en nuestra recolección de datos.

Las grandes filtraciones del año 2010, pero sobre todo el *Cablegate*, supusieron un cambio clave en la estrategia de WikiLeaks, fundamental para darse a conocer a la opinión pública mundial, al encomendar su alijo de secretos a la prensa tradicional más influyente, renunciando a su simple publicación en bruto en el sitio web de WikiLeaks y otorgando exclusividad —aunque limitada en el tiempo— a un grupo reducido de medios. En el caso del *Cablegate* —que marcó el apogeo de WikiLeaks—, pese a que sólo unos pocos cables diplomáticos pasaron por el filtro de la edición periodística, el impacto de WikiLeaks con aquellas publicaciones diseñadas en las redacciones de *The Guardian*, *The New York Times*, *Der Spiegel*, *Le Monde* y *El País* fue notablemente mayor que el logrado tras la publicación en la página web de WikiLeaks de la totalidad

de los 251.287 cables diplomáticos filtrados, una vez rotas las relaciones con estos cinco periódicos.

En el año 2011 se inició la tercera etapa de WikiLeaks, tras la ruptura de relaciones con los medios con los que había colaborado hasta entonces. Después de un agrio debate público con sus excolaboradores, en el que subyacía la tensión entre el modelo periodístico tradicional y los valores de la ética hacker, WikiLeaks emprendió un nuevo camino con una mayor variedad de socios. La nueva estrategia se consolidó en el año 2012, con colaboraciones más abiertas, dando acceso a sus archivos a periodistas independientes, científicos y activistas. Por volumen de documentos, los conocidos como *GI Files* —más de cinco millones y medio de correos electrónicos de la agencia de inteligencia Stratfor— fueron la mayor filtración hecha, pero lo cierto es que ni con ésta ni con ninguna otra WikiLeaks alcanzó los niveles de popularidad y de impacto logrados en el año 2010, principalmente con el *Cablegate*.

Todas estas filtraciones sirvieron además como aprendizaje para algunos medios y periodistas, y como inspiración para nuevos confidentes, contagiándose por todo el mundo un nuevo modelo de periodismo de filtraciones basado en el uso de alta tecnología segura, la Red y sistemas sofisticados para el manejo de grandes volúmenes de documentos y datos. Así, por ejemplo, las revelaciones de Edward Snowden sobre los sistemas de espionaje global del Gobierno estadounidense —la filtración más sustancial en décadas— se deben a la experiencia previa de WikiLeaks y al ejemplo del soldado Manning. Esta exclusiva fue compartida por los periódicos *The Guardian* y *The Washington Post* —que colaboraron antes con WikiLeaks— y les sirvió para ganar el premio Pulitzer en el año 2014, en la categoría de servicio público, un galardón que supone un reconocimiento al periodismo colaborativo inspirado por la cultura hacker.

Cuarta

El objetivo principal de Julian Assange es conseguir el máximo impacto político en Occidente mediante la geoposición, multiplicación y viralización del mensaje. De ahí su primera selección para el *Cablegate* de los cinco medios de comunicación a los que ofreció en exclusiva los cables diplomáticos, cuatro europeos y uno norteamericano: los diarios *The New York Times* (Estados Unidos), *The Guardian* (Reino Unido), *Le Monde* (Francia) y *El País* (España), además del semanario *Der Spiegel* (Alemania). Cinco

periódicos globales e influyentes que se editan en los cuatro idiomas más populares y poderosos, política y económicamente, en el mundo occidental: inglés, francés, español y alemán.

Assange se valió de estos medios para lograr sus objetivos en América y Europa, que es donde se juega el prestigio y crédito de WikiLeaks y el suyo personal, y se aseguró algunas protecciones legales, parapetándose tras el derecho a la libertad de prensa de sus socios. A cambio, Assange ofreció a estos medios una ventaja competitiva en sus mercados: la exclusividad, un salvavidas en un momento crítico para la prensa tradicional, que vive su mayor crisis de credibilidad y de negocio. Rotas las relaciones con estos medios, WikiLeaks intentó compensar su pérdida de influencia ampliando el abanico de medios colaboradores e integrando a periodistas independientes, académicos y activistas en la producción, publicación y difusión de investigaciones basadas en sus filtraciones.

Quinta

Las distintas estrategias ejecutadas por WikiLeaks para publicar documentos secretos y los datos de impacto obtenidos en nuestra investigación evidencian que la idea primigenia de Julian Assange de liberar la información masivamente y en bruto en su sitio web, sin pasar por el filtro de los procesos periodísticos y de los medios convencionales, fracasó por su ineficacia para influir en la opinión pública y para causar reacciones sociales y políticas significativas. WikiLeaks tuvo que recurrir a las labores clásicas del periodismo y a los medios convencionales para asistir informativamente a las masas no ilustradas en el acceso, búsqueda, verificación, tratamiento, análisis e interpretación de información y datos en bruto, cuya simple liberación no es eficaz para impactar en la opinión pública.

El fenómeno WikiLeaks demuestra que los procesos periodísticos clásicos siguen siendo claves para que los ciudadanos dispongan de información contrastada, digerible y útil, que sea comprensible y de fácil acceso. Al abrir sus bases de datos a cada vez más periodistas e investigadores, WikiLeaks reconoció su incapacidad de gestionar y procesar la ingente cantidad de información que acumula, admitiendo asimismo la dificultad que supone también para los ciudadanos enfrentarse a enormes volúmenes de documentos y de datos en bruto. Al mismo tiempo, WikiLeaks asumió

que las labores clásicas del periodismo y la capacidad de difusión y de influencia de la prensa clásica siguen siendo fundamentales para alcanzar su objetivo de máximo impacto político.

La estrategia del máximo impacto mediático para conseguir el máximo impacto político llevó así a WikiLeaks a renunciar en un primer momento a algunos principios de la ética hacker y a acatar el papel de *gatekeepers* de los periodistas y del propio Gobierno de Estados Unidos. WikiLeaks se consagró de este modo al modelo periodístico tradicional de selección, edición, jerarquización y comercialización de información exclusiva, en colaboración con cinco grandes organizaciones tradicionales de noticias.

Sexta

La popularidad de WikiLeaks y su influencia política dependen de su impacto en los medios tradicionales de masas más influyentes en Occidente. Los picos más altos de popularidad de la organización en Internet coinciden con su máximo impacto en los cinco grandes medios que colaboraron en el *Cablegate*: *The New York Times*, *The Guardian*, *Le Monde*, *Der Spiegel* y *El País*. Rotas las relaciones con estos medios, y a pesar de intensificar su actividad en las redes sociales durante 2011 y 2012, WikiLeaks no logró igualar las cotas de popularidad y el impacto conseguido a finales de 2010. Y está lejos de conseguir el grado de aceptación e influencia social de su principal antagonista, Facebook, pese a los esfuerzos de Assange por competir con esta compañía, concentrados en el fracasada red social WLFriends.

En 2010, Julian Assange entendió que necesitaba exponer masivamente en los medios periodísticos convencionales los documentos secretos que poseía WikiLeaks para hacer popular a su organización, lograr el máximo impacto político e influir en el debate público global. Y esto sólo era posible con el máximo impacto mediático. Cuanto mayor fuese el acceso a los ciudadanos y el impacto en la opinión pública, mayor sería el impacto político. El máximo impacto no sólo se alcanzaría, pues, con la publicación en el sitio web de WikiLeaks de una cantidad ingente, sin precedentes, de material confidencial, sino también, y sobre todo, articulando una cooperación histórica entre algunas de las mayores organizaciones de noticias del mundo, que a la vez reportaron legitimidad ante la opinión pública y popularidad a WikiLeaks.

La colaboración sin precedentes en el *Cablegate* de cinco medios de comunicación generalistas globales, tradicionales e influyentes fue decisiva en la legitimación, popularización e impacto en la esfera pública de WikiLeaks y de Julian Assange. Con los datos obtenidos, podemos asegurar que hay una relación causal entre el impacto de las filtraciones en los medios de masas y el impacto sociopolítico, y también académico, de WikiLeaks.

El cotejo de los datos de la actividad de WikiLeaks y de su impacto en Internet demuestran que una mayor actividad de esta organización en las principales redes sociales en línea no obtuvo como resultado una mayor respuesta por parte del público ni, por lo tanto, un mayor impacto. A pesar de que en 2011 la organización alcanzó su actividad más intensa en redes sociales, o de que en 2012 inició una experiencia colaborativa más amplia y diversa con nuevos colaboradores, fue en 2010 cuando WikiLeaks obtuvo su mayor impacto e influencia en Internet gracias a la difusión que le dieron medios dominantes, alcanzando sus picos más altos durante las publicaciones de los cables diplomáticos de Estados Unidos, en una colaboración sin precedentes entre cinco de los medios de masas más influyentes en Occidente. Esta difusión también contribuyó a que creciese el impacto de WikiLeaks en la literatura científica.

Tras romperse la alianza con estos medios, en febrero de 2012 WikiLeaks intentó repetir la experiencia con un acuerdo de colaboración con veintinueve organizaciones heterogéneas, repartidas por los cinco continentes, que luego amplió a más colaboradores, en la filtración masiva conocida como *The Global Intelligence Files*. Sin embargo, lejos de conseguir resultados semejantes, el efecto WikiLeaks y el impacto de su mensaje fue menor y se desvaneció más rápidamente.

Séptima

Más ampliamente, en la era de Internet y de la sociedad red, de una sociedad hiperconectada por redes electrónicas, los medios de masas siguen siendo claves para lograr el máximo impacto de un mensaje.

De los datos obtenidos en nuestra investigación y de su análisis colegimos que existe una gran dependencia de los comportamientos de los usarios de Internet a la agenda de los medios de masas, que siguen estableciendo los grandes temas sobre los

que debe pensar el público. La alta correlación entre los momentos de máxima difusión de noticias sobre WikiLeaks en los medios dominantes y los picos más altos en las búsquedas de información en la Red sobre esta organización (en el buscador de Google, en las visitas a la página web de WikiLeaks, en el seguimiento en sus redes sociales y en las consultas a su página en Wikipedia) demuestra que los medios de comunicación de masas siguen teniendo una gran influencia sobre el público, al determinar qué historias tienen interés informativo y durante cuánto tiempo deben permanecer en el centro del debate público.

En nuestra investigación comprobamos que la difusión de acontecimientos relacionados con WikiLeaks por parte de los medios dominantes influye en todos los niveles de comportamiento y en todos los espacios virtuales de búsqueda de información, participación, afiliación, difusión y narración en Internet, relacionados con esta organización.

También constatamos dinámicas de retroalimentación entre los distintos ciberentornos por los que transitan los internautas, de manera que la misma información esparcida en los espacios virtuales de confluencia masiva circula de un lugar a otro en Internet con los mismos niveles de intensidad.

Los datos obtenidos en nuestro caso de estudio muestran una altísima correlación entre el comportamiento en las búsquedas en Google sobre WikiLeaks, el flujo de visitas al sitio web y al *wiki* de esta organización, su impacto e influencia en las redes sociales en línea y el interés generado en la producción del relato popular sobre esta organización en Wikipedia, todo ello condicionado por la agenda de los medios dominantes.

Estas correlaciones demuestran que Internet, como metamedio, genera dinámicas de confluencia entre los distintos espacios virtuales de búsqueda, publicación, difusión y seguimiento de la información, fomentando procesos simultáneos y complementarios que favorecen tendencias virales en la Red.

Octava

En nuestra experiencia en las filtraciones de los correos electrónicos de Stratfor comprobamos la gran dificultad, la complejidad y el enorme trabajo y dedicación que

implica tratar alijos de información confidencial tan grandes como los que provee WikiLeaks. Y constatamos la necesidad que tiene esta organización de ampliar su red de colaboradores para dar salida a toda la información que guarda y conseguir la mayor cobertura y difusión posibles.

Tras el gran impacto del *Cablegate* y la discreta repercusión de las filtraciones que siguieron, WikiLeaks tuvo que dar un nuevo giro a su estrategia en 2012, tras las primeras publicaciones de los correos de Stratfor, ampliando su red de colaboradores mediante un sistema de invitaciones personales a periodistas independientes, académicos y activistas, a los que dio acceso a su base de datos de los *GI Files* para ampliar la cobertura informativa del enorme alijo de documentos que guardaba, de los que apenas un uno por ciento había sido publicado en cinco meses por las veintinueve organizaciones que inicialmente fueron seleccionadas para estas filtraciones.

De nuestra observación participante concluimos también que WikiLeaks permite a los periodistas trabajar con plena autonomía, sin injerencias de ningún tipo ni condiciones que comprometan su libertad en todo el proceso periodístico, desde la selección de los temas noticiables y de los materiales, hasta la publicación y difusión de la noticia, pasando por el tratamiento y edición de la información y su contextualización para hacerla digerible para el público.

El único control, mínimo, que impone WikiLeaks es sobre la publicación de la información, que debe ser coordinada entre ambas partes para operar con la máxima eficacia y eficiencia en el proceso de difusión. Así, el investigador debe incorporar previamente una referencia y enlace a su publicación en los registros de WikiLeaks para dar contexto y explicación al material en bruto, que se libera en el sitio web de esta organización al mismo tiempo que el investigador hace público su trabajo, de manera que la información editada y los documentos en bruto se publican y se difunden por distintos canales simultáneamente.

Estamos, por lo tanto, ante un modelo híbrido en el que la información en bruto y la información editada se publican de manera sincronizada y enlazada para que cualquier individuo tenga acceso a una versión digerible de los contenidos de los documentos filtrados y a la vez pueda cotejar la información en bruto y la editada, además de poder usar libremente los documentos originales una vez liberados.

Novena

De nuestra investigación participante y de nuestro análisis de las filtraciones de WikiLeaks inferimos que, en una sociedad global estructurada en red, la exclusividad sobre grandes volúmenes de información y de datos es insuficiente y contraproducente para la pluralidad informativa, la transparencia y la libre circulación de información. El concepto periodístico de exclusividad, entendido como exclusión y, por lo tanto, como privación a otros de acceso a los materiales y recursos informativos, contradice los ideales hackers, contrarios a la existencia de derechos exclusivos y privativos sobre la información.

Con su cambio de estrategia en 2010, WikiLeaks renegó de principios básicos de la ética hacker, otorgando acceso exclusivo a la información a un grupo reducido de medios. Y si bien es cierto que comprobamos que el *Cablegate* consiguió los mayores niveles de impacto para el fenómeno WikiLeaks, fue más un éxito publicitario que informativo, tanto para esta organización como para los propios medios que gozaron de la exclusiva.

La estrategia de exclusividad consiguió el objetivo de máximo impacto sociopolítico, pero se mostró fallida en cuanto al tratamiento y cobertura informativa. Lo mismo sucedió con las filtraciones de Stratfor, en las que en un principio se diseñó otro sistema de privación en el acceso a la información, exclusivo primero para veintinueve socios, pero que también se mostró errado en la cobertura informativa, lo que llevó finalmente a WikiLeaks a ampliar su red de colaboradores mediante un sistema de invitaciones confidencial, pero no excluyente, sino abierto, otorgando a sus nuevos colaboradores la capacidad de dar ellos mismos acceso a la información a otros investigadores de diferentes medios y organizaciones, mediante un sistema de invitaciones personales.

De esta manera, WikiLeaks recuperó sus principios hackers y permitió que la información pudiese estar al alcance de toda una variedad de periodistas, académicos y activistas, asegurando así una mayor libertad y pluralidad en el tratamiento de la información, y una mayor amplitud a su difusión y diversidad a su uso.

Con esta nueva estrategia, WikiLeaks abrió además la participación a medios alternativos y regionales, y a lenguas no dominantes, incluyéndolos en la narración de las mayores filtraciones de la historia hasta ese momento, quedando demostrada, tras

nuestra experiencia en las filtraciones de Stratfor, la importancia que los fenómenos globales y la liberación masiva de información y de datos, en una sociedad estructurada en red, tienen para las comunidades locales o regionales y sus medios de comunicación, cuyos conocimientos e intereses particulares son también un valor añadido a estos procesos de liberación masiva de documentos y archivos a escala global.

Décima

El medio —WikiLeaks— es el mensaje, y el mensaje es subvertir la estructura tradicional de los poderes político y mediático, y desmantelar el secreto como mecanismo de control y manipulación de la realidad por parte de los Estados-nación y de las grandes corporaciones. Tanto en las filtraciones del *Cablegate* como en las de los *GI Files* —analizadas en nuestra investigación— el mensaje principal es la demostración de poder de WikiLeaks y del periodismo hacker, al introducirse en el sistema nervioso de gobiernos y de empresas poderosas, sustraer su información secreta y organizar colaboraciones sin precedentes en la historia del periodismo para hacer públicos esos secretos.

A la vez, WikiLeaks está cuestionando el papel que los medios de información mercantilizados y sus periodistas juegan como correas de transmisión de los poderes político y económico, aun cuando WikiLeaks haya recurrido precisamente a ellos para lograr su último objetivo: el máximo impacto político. WikiLeaks actúa como una suerte de Caballo de Troya contra las corporaciones mediáticas y como acicate para los periodistas que quieren liberarse de las ataduras a los poderes político y corporativo, dotándolos de las herramientas necesarias para alcanzar su plena soberanía.

En todo ello subyace, además, un mensaje que es una alerta a la sociedad: ya no podemos seguir fingiendo que no sabemos y, por lo tanto, estamos moralmente obligados a defender activamente los derechos de libre expresión, libre circulación de la información, acceso universal al conocimiento y privacidad del individuo, amenazados por un sistema de vigilancia y control global.

El mayor valor de las filtraciones de WikiLeaks reside, por lo tanto, en la exhibición de poder que demostró esta organización ante la autoridad, en su mensaje ejemplarizante a los medios periodísticos y en su aviso a la opinión pública de que

tenemos derecho a conocer cómo funcionan nuestros gobiernos y a tener acceso a la información de interés público que manejan en secreto éstos y las grandes corporaciones, como son los correos y documentos que publicamos en nuestra participación en las filtraciones de los *GI Files*.

Undécima

Los medios de comunicación convencionales ayudaron a desviar la atención del mensaje (WikiLeaks) y de sus implicaciones sociopolíticas (libertad de información y transparencia), y contribuyeron a centrar la atención en el mensajero (Julian Assange). Esto se hace evidente en nuestro análisis de las portadas publicadas por los medios colaboradores de WikiLeaks durante el primer mes del *Cablegate*, que confirma los resultados del estudio *Getting Personal: Personification vs. Data-Journalism as an International Trend in Reporting about Wikileaks* (Czepeck, 2011), que apuntan a que la atención mediática a las filtraciones de WikiLeaks cayó de forma abrupta tras la primera semana de publicaciones y que *The Guardian* fue, de los cinco medios asociados, el que más importancia dio a los cables diplomáticos de Estados Undidos

En nuestro análisis comprobamos que el apogeo del fenómeno WikiLeaks se produjo el 29 de noviembre de 2010, cuando se anunció a bombo y platillo el inicio del *Cablegate*. Tras este éxtasis, más publicitario que periodístico, las noticias basadas en los documentos de las filtraciones apenas aguantaron cuatro días casi monopolizando las portadas de los periódicos. A partir de ahí, fueron empequeñeciéndose progresivamente, hasta desaparecer de las primeras páginas de los periódicos en apenas un mes, con pequeños repuntes que coincidieron con el caso judicial de Julian Assange.

Los medios fueron rápidamente desviando la atención del mensaje y empezaron a centrarla en el mensajero, en la personalidad y en la vida del fundador de WikiLeaks, novelizada en dos apresurados libros publicados por *The Guardian* y *The New York Times* a finales de enero de 2011, cuando la inmensa mayoría de los cables diplomáticos se mantenían ocultos a la opinión pública. Pero a ello también contribuyó el propio Julian Assange, quien se colocó en el centro de la diana en el año 2010, cuando WikiLeaks empezó a ser popular. Hasta entonces, Assange había preferido mantenerse en un segundo plano, incluso en el anonimato. Por ejemplo, tras revisar las primeras publicaciones sobre WikiLeaks en los medios, en enero de 2007, comprobamos que en

éstas no se hizo ni una sola mención a Assange, un auténtico desconocido fuera de los círculos hackers, quien por entonces prefirió mantener oculta su identidad, al igual que sus colaboradores, para asegurar el proyecto y a sus actores. Sin embargo, Assange se convirtió en el protagonista central en 2010, iniciándose un proceso sinecdocal que llevó a WikiLeaks a convertirse en Assange, y a Assange en WikiLeaks.

Duodécima

La historia de Julian Assange es el resultado de la aplicación de estrategias narrativas transmediáticas destinadas a convertir al líder de WikiLeaks en héroe o villano, según el tradicional sistema de antinomias u oposiciones binarias que han contrbuido a organizar una comprensión y evaluación social del hacker y del hacktivismo. En esta lucha dialéctica participaron tanto sus defensores y detractores como el propio Julian Assange. Además, los medios colaboradores en el *Cablegate* aplicaron estrategias de *storytelling* para *matar* al mensajero, solapando el mensaje, el valor sociopolítico de las filtraciones y el papel que juega WikiLeaks como nuevo intermediario en el ecosistema informacional. Como hemos analizado y explicado, los discursos político y mediático se centraron en la figura del fundador de WikiLeaks y ahondaron de manera sesgada en su intrincada personalidad, en sus aventuras y desventuras, en sus obsesiones y en el halo de misterio que le rodea, sin aplicar un análisis riguroso y profundo que aclarase las auténticas raíces ideológicas y culturales que explican sus motivaciones, que se hallan en el mismo proceso evolutivo de la cultura hacker y en su ética alternativa. Estos discursos basados en cuestiones éticas y estéticas propias de la moral dominante desenfocaron la atención sobre el mensaje ulterior —el desmantelamiento del Estado de secreto— y sobre los datos y hechos.

La historia —o *wikistory*— de Julian Assange es paradigma también de las nuevas narrativas transmediáticas, que contribuyen a expandir el universo WikiLeaks por el espacio físico y el espacio cíber mediante procesos de convergencia mediática, cultura participativa e inteligencia colectiva. WikiLeaks obligó además a los *spin doctors* a renovar sus tácticas de *storytelling* para un fenómeno transmediático, transnacional y transversal.

La universalización del acceso a Internet, la irrupción de nuevos medios de comunicación alternativos que permite la Red, el abaratamiento de la tecnología digital

y la democratización de las herramientas de producción y distribución de la información, han permitido que aparezcan nuevos autores y voces que contribuyen a construir nuevos relatos que difieren de la versión oficial dominante e incluso la contradicen, compitiendo en los mismos espacios.

A las colaboraciones puntuales y estratégicas con medios convencionales dominantes para difundir el mensaje, WikiLeaks sumó a su causa innumerables apoyos y contribuciones en blogs, redes sociales, foros de Internet y medios alternativos para la contrainformación y el contrapoder, y consiguió el soporte de toda una variedad de individuos, colectivos y organizaciones civiles y políticas cuyas acciones y discursos se desarrollan a la par en el ciberespacio y en ciudades de todo el mundo. Esta red hiperespacial hace fluir permanentemente el mensaje de WikiLeaks y sus filtraciones, y expande el universo WikiLeaks por el espacio físico y el espacio cíber.

La historia de Julian Assange y de WikiLeaks es, en definitiva, un caso manifiesto de aplicación de técnicas del *storytelling* para crear la primera gran *wikistory* en la era de la sociedad red, en la que Assange ha ejercido como el gran hacedor de la que puede ser considerada la más vibrante y apasionante historia periodística de la primera década del siglo XXI y la más publicitada desde el *Watergate* como hito del periodismo, resultado de un nuevo paradigma comunicacional caracterizado por la convergencia mediática, la cultura participativa y la inteligencia colectiva.

Decimotercera

A principios de la década de 1990, los hackers alertaron del poder de persuasión de los medios de comunicación de masas y de su capacidad para hacer creíble cualquier relato y darle sello de verdad universal, incluido el que convierte a los hackers en criminales. Dos décadas después, los hacktivistas disponen de poderosas herramientas para replicar el discurso de los medios institucionalizados e intentar contrarrestar su poder. La popularización de la Red de redes y la democratización de las tecnologías de la información y la comunicación han permitido equilibrar las fuerzas entre un bando movido por el capital y el derecho al secreto, y otro motivado por la cooperación sin ánimo de lucro, la transparencia institucional y el derecho a la privacidad del individuo. WikiLeaks, desde su propia página web y desde sus canales en las redes sociales en línea, ha contribuido a este nuevo equilibrio de poder.

Buen ejemplo de ello fue la disputa dialéctica que WikiLeaks mantuvo con los cinco medios colaboradores en el *Cablegate* a principios de septiembre de 2011, cuando la organización de filtraciones decidió publicar todos los cables diplomáticos de Estados Unidos sin pasar previamente por el filtro periodístico. Sin embargo, dado que WikiLeaks no goza ni de las protecciones legales ni de la legitimidad, crédito y autoridad social de los que sí disfrutan los medios tradicionales y sus periodistas, se ve obligada a dar más explicaciones sobre sus acciones y motivaciones. Esto lo comprobamos en el análisis de los textos publicados por WikiLeaks y *The Guardian* en su crisis, en los que observamos que la organización de filtraciones necesita exponer más información, datos, contexto y argumentos que los medios opositores para convencer a la opinión pública.

En nuestro análisis de contenido también verificamos que formalmente el discurso de WikiLeaks no tiene nada que envidiar al de los medios periodísticos pero, sobre todo, que estos últimos están más interesados en inocular una opinión negativa sobre WikiLeaks como una amenaza, mientras que la organización hacktivista parece articular un discurso más neutral, en el que tiene más peso la información que la opinión y donde el concepto positivo de seguridad se contapone al negativo de amenaza que impregna el relato de *The Guardian* como cabecilla de los cinco medios que se aliaron en el *Cablegate*, reproduciéndose una vez más la ya clásica lucha dialéctica entre la ética hacker y la moral dominante. Corroboramos, además, que existe una necesidad por ambas partes de personalizar el conflicto, centrando sus discursos en Julian Assange y en el periodista David Leigh, para dañar su credibilidad y, por extensión, la reputación de las organizaciones a las que representan.

Por último, consideramos que el discurso de WikiLeaks es más constructivo para la crítica y el análisis de la profesión periodística y para su reconfiguración como instrumento de defensa de los derechos humanos, en oposición al papel central que juegan hoy los medios periodísticos en la promoción de diferentes intereses políticos y corporativos.

Decimocuarta

Podemos concluir que el fenómeno WikiLeaks ofrece nuevos paisajes en la economía política de la comunicación, contribuye además de manera sustancial al análisis crítico

del papel de los medios en los procesos de cambio social y plantea los retos más importantes que debe afrontar el periodismo en la sociedad red y en un nuevo orden global de control y vigilancia masiva.

CONSIDERACIONES FINALES DEL AUTOR Y FUTURAS INVESTIGACIONES

A modo de corolario, consideramos necesario destacar, con la experiencia y el aprendizaje que hemos ganado en esta investigación, que el espíritu hacker de hoy es esencialmente el mismo que el de hace seis décadas. En esta travesía por la cultura hacker, desde los primeros *hacks* en el Massachusetts Institute of Technology hasta las filtraciones de documentos secretos de WikiLeaks, hemos notado el espíritu inquieto y curioso, la pasión, la libertad, la creatividad y la alegría que caracterizan a los hackers, pero también la dimensión política que siempre ha existido en en el *hacking*, que se manifiesta en la oposición a la autoridad y a cualquier tipo de censura, en la defensa de la libre información y la promoción de la transparencia, en la libertad del individuo para explorar y conocer, en la voluntariedad como principio básico de actuación y en la cooperación directa como fuente de progreso individual y colectivo. Hackear no es algo malo, no es un acto destructivo, todo lo contrario; hackear, en su sentido genuino, significa progreso. Los hackers informáticos han contribuido de manera decisiva al desarrollo tecnológico y los hacktivistas han aplicado el *hacking* para el progreso y la justicia social. Ahora, en WikiLeaks vemos un intento de realizar el mayor *hack* de la historia, hackeando el sistema en sí mismo; un *hack* supremo que infunde tanto temor como fascinación.

No podemos concluir esta tesis sin subrayar que la censura, el bloqueo, la penalización y el castigo a WikiLeaks y a Julian Assange soporta el mismo mensaje que se envió en 1990, cuando se acosó al editor del boletín de noticias *Phrack*, o en el año 1999, cuando se actuó contra la revista *2600*. Ni WikiLeaks ni Julian Assange son las primeras ni serán, probablemente, las últimas víctimas del acoso institucional a la cultura hacker, cuyos medios de comunicación son marginados y boicoteados por un sistema que decide selectivamente qué es periodismo y quién está protegido por las leyes que amparan a los periodistas y editores de medios. Los ataques a *Phrack*, a *2600* o a WikiLeaks han supuesto un atentado en toda regla contra el derecho a la libertad de prensa y de información, derechos que parece haberse arrogado en exclusiva la prensa convencional, lo cual supone una privatización de derechos básicos contraria a una sociedad libre y plural.

Sin embargo, existe una diferencia sustancial entre los casos precedentes de

acoso a todo cuanto oliese a hacker y el que nos ocupa ahora, y es el enorme soporte económico, tecnológico, mediático y legal conseguido por la organización de Julian Assange, a escala global. Si en 1990 las grandes redadas contra los hackers en Estados Unidos originaron la primera acción política y solidaria hacktivista en red en defensa de la libre información y la auténtica libertad de prensa, a escala nacional, que dio como fruto el nacimiento de la primera organización política del ciberespacio, la Electronic Frontier Foundation, lo que vemos ahora es que Julian Assange está liderando la primera gran acción política y solidaria hacktivista en red en defensa de la libre información, la libertad de prensa y los derechos humanos, a escala global, con WikiLeaks como catalizador de esas preocupaciones cada vez más extendidas en la contracultura digital, trasladando su mensaje por todos los rincones del espacio cíber y del espacio real a través de experiencias transmediáticas y de la acción física y virtual de individuos, colectivos y organizaciones que funcionan como nodos interconectados en una red hiperespacial electrizada por los nuevos *watchdogs* y sus correligionarios.

Con la *institucionalización* de la ética hacker, a partir de principios de la década de 1990 —con la Electronic Frontier Foundation como ariete— y el uso cada vez más intenso de medios de comunicación sociales en línea, los hackers salieron de la clandestinidad. El culmen de este proceso de *civilización* y *normalización* hacker ha sido la aparición de WikiLeaks como actor institucionalizado en las esferas mediática y política, y como actor influyente en los foros públicos de debate, logrando que gobiernos, corporaciones y medios convencionales se mantengan en un estado de alerta permanente y pierdan el espacio de confort en el que se habían instalado.

Que WikiLeaks sobreviva o no en los próximos años nos parece, sin embargo, una cuestión secundaria. El asunto central, sobre el que pretendemos desarrollar futuras investigaciones, es cómo se resolverá el desafío de la ética hacker al espíritu dominante en la sociedad red, cómo se solventará la tensión entre el modelo hacker de sociedad abierta —basada en la libre información, el intercambio de conocimiento, la transparencia, el derecho a la privacidad y el bien común— y el modelo autoritario de control de las redes de comunicación y de privatización de la información y del conocimiento. Consideramos que esto dependerá, en buena medida, de que se tomen las experiencias hackers, incluida la de WikiLeaks, como un aprendizaje o como meros accidentes.

Nuestra intención es seguir indagando en los procesos impregnados por la ética y la cultura hackers, así como contribuir a aplicar sus valores en el campo académico y aportar una lectura crítica desde nuestro campo de investigación —los medios de comunicación— a una composición transversal sobre los nuevos mecanismos de comunicación, información, control y poder en la sociedad red, en la que participen hackers, periodistas, programadores, matemáticos, filósofos, sociólogos, politólogos, artistas, etc. Como si de una nueva vacuna en fase de pruebas se tratase, creemos que es necesario contribuir a estudiar y comprobar la seguridad, la eficacia y los efectos secundarios de la aplicación de la ética hacker como vacuna contra los males del poder en la sociedad red.

RECOMENDACIONES

Primera

Aconsejamos a las nuevas generaciones de periodistas y a aquellos profesionales que aún sientan pasión por el periodismo que se empapen de cultura hacker, que hagan suyos los valores de la ética hacker y que interactúen y colaboren con comunidades hackers. Consideramos que la emergencia de la figura del periodista hacker y de una ética periodística hacker contribuirán de manera decisiva a la defensa de la libertad de expresión y de información, a reinventar el periodismo y los medios de información y, por lo tanto, a asegurar la salud de la democracia, permanentemente amenazada.

Segunda

Es necesario y urgente que los periodistas se familiaricen con distintos lenguajes de programación y los dominen como un lenguaje natural. Creemos que es básico que los profesionales de la información adquieran habilidades computacionales para comprender la evolución que ha tenido la sistematización de tareas y el manejo de la información mediante la computación, para que refuercen y estimulen un pensamiento lógico, para que adquieran la soberanía necesaria para manejarse en las redes electrónicas, para que puedan trabajar con solvencia con grandes cantidades de datos y para que tengan la capacidad de desarrollar o mejorar software para sus investigaciones.

Tercera

A los medios de información y a los periodistas, y a la sociedad en general, recomendamos que implementen sistemas de encriptación en sus dispositivos tecnológicos para una comunicación segura y privada. En el caso de los profesionales de la información, para proteger su libertad frente al potencial control de sus comunicaciones, para garantizar la confidencialidad de éstas, para proteger también a sus fuentes y para generar la confianza necesaria para que los secretos fluyan y broten. A los usuarios de tecnologías conectadas a la Red aconsejamos que implementen sistemas de encriptado para evitar el rastreo de sus comunicaciones electrónicas y pàra

asegurar su privacidad. Consideramos que la encriptación no puede ser un derecho reservado y que todo el mundo debe conocer y poder utilizar sistemas de cifrado.

Cuarta

Consideramos también necesario que las universidades desarrollen e implementen software libre y de código abierto para avanzar en un modelo de investigación en red, abierto y comunitario, del que se beneficie toda la comunidad académica.

Quinta

Proponemos a la Universidad Carlos III crear un laboratorio hacker (*hacklab*) abierto a estudiantes, profesores, investigadores y profesionales de la comunicación y de la información, de la computación, de las telecomunicaciones y de las nuevas tecnologías y artes digitales o electrónicas, para que puedan compartir experiencias y conocimientos, y para que pongan en marcha proyectos abiertos de investigación, desarrollo e innovación.

Sexta

Solicitamos a la Real Academia Española que retire la definición dada en su diccionario al término *hacker* y que le conceda su significado genuino, y a los profesionales de los medios de información, que no sigan contribuyendo a confundir a la sociedad en el uso de la palabra *hacker* y eviten su utilización como sinónimo de criminal o delincuente informático.

REFERENCIAS

Ackerman, B. (2011, 15 de marzo). A Statement on Private Manning's Detention. *Balkinization*. Disponible en: <http://balkin.blogspot.com.es/2011/03/statement-on-private-mannings-detention.html> [Consulta: 15 de diciembre de 2013).

Adams, J. (1998). *The Next World War: Computers Are the Weapons and the Fron Line is Everywhere*. New York: Simon & Schuster.

Aftergood, S. (2007, 3 de enero). Wikileaks and Untraceable Document Disclosure. *Secrecy News*. Federation of American Scientists. Disponible en: <http://fas.org/blogs/secrecy/2007/01/wikileaks_and_untraceable_docu/> [Consulta: 2 de junio de 2014].

Agencias. (2011, 21 de enero). Julian Assange, la película. *El País*. Disponible en: <http://elpais.com/elpais/2011/01/21/actualidad/1295596131_850215.html> [Consulta: 20 de diciembre de 2011].

Agencia EFE. (2007, 11 de enero). Wikileaks pone voz a la disidencia china en Internet. *El País*. Disponible en: <http://tecnologia.elpais.com/tecnologia/2007/01/11/actualidad/1168507683_850215.html> [Consulta: 18 de abril de 2014].

Agencia EFE. (2007, 12 de enero). 'WikiLeaks' desafía a la censura en Internet. *El Mundo*. Disponible en: <http://www.elmundo.es/navegante/2007/01/11/tecnologia/1168530229.htm> [Consulta: 18 de abril de 2014].

Agencia EFE. (2010, 14 de diciembre). Julian Assange, rockero del año. *ABC*. Disponible en: <http://www.abc.es/20101213/cultura-musica/assange-rockero-201012131625.html> [Consulta: 2 de diciembre de 2011].

Alandete, D. (2011, 12 de marzo). Twitter deberá revelar a EEUU información sobre WikiLeaks. *El País*. Disponible en: <http://tecnologia.elpais.com/tecnologia/2011/03/12/actualidad/1299924061_850215.html> [Consulta: 15 de febrero de 2014].

Almirón Roig, N. (2007). La economía política de la investigación informacional. *Revista Latina de Comunicación Social*, Vol. 10, No 62. Laguna, Tenerife. Disponible en: <http://www.ull.es/publicaciones/latina/200716Almiron.htm> [Consulta: 15 de diciembre de 2012].

Anderson, C. (2004, 24 de octubre). The Long Tail. *Wired*. Disponible en: <http://www.wired.com/wired/archive/12.10/tail.html> [Consulta: 12 de febrero de 2013].

Andrejevic, M. (2014). WikiLeaks, Surveillance, and Transparency. *International Journal of Communication*, 8, pp. 2619–2630.

Andrews, J. (ed.) (2011). *The Wikileaks-Movie.com Project*. California: Imagine Publishing, Inc. Disponible en: <http://wikileaks-movie.com/> [Consulta: 30 de noviembre de 2011].

Androutsellis-Theotokis, S. y Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, Vol. 36, No. 4, pp. 335–371.

Angwin, J. (2011, 10 de octubre). Secret Orders Target Email. *The Wall Street Journal*. <http://www.wsj.com/articles/SB10001424052970203476804576613284007315072> [Consulta: 16 de febrero de 2014].

Anonymous leaks in the Internet age. (2007, 18 de enero). *The Minnesota Daily*. University of Minnesota. Disponible en: <http://www.mndaily.com/2007/01/18/anonymous-leaks-internet-age> [Consulta: 16 de abril de 2014].

Association for Progressive Communications. (2001, 1 de febrero). *History*. Disponible en: <https://www.apc.org/en/about/history> [Consulta: 18 de octubre de 2014].

Arias, J. (2010, 9 de diciembre). Lula dice que la detención de Assange "atenta contra la libertad de expresión". *El País*. Disponible en: <http://www.elpais.com/articulo/internacional/Lula/dice/detencion/Assange/atenta/libertad/expresion/elpepuint/20101209elpepuint_18/Tes> [Consulta: 12 de diciembre de 2012].

Arquilla, J. y Ronfeldt, D. (1993). Cyberwar Is Coming! En Arquilla, J y Ronfeldt, D (eds.) (1997), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 23-60). Santa Monica, California: RAND Corporation.

Arquilla, J. y Ronfeldt, D. (1999). *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica, California: RAND Corporation.

Arquilla, J. y Ronfeldt, D. (eds). (2001). *Networks and netwars: The Future of Terror, Crime and Militancy*. Santa Monica, California: RAND Corporation.

Assange, J. (2006, 8 de junio - 2007, 29 de agosto). *Selected Correspondence*. Disponible en: <http://web.archive.org/web/20071020051936/http://iq.org/ > [Consulta: 8 de diciembre de 2011].

Assange, J. (2006, 3 de diciembre). *Conspiracy as Governance*. Disponible en: <http://web.archive.org/web/20070829163014/http://iq.org/conspiracies.pdf > [Consulta: 8 de diciembre de 2011].

Assange, J. (2011). *Julian Assange: The unauthorised autobiography*. Edinburgh: Canongate Books.

Assange, J. (2014). *When Google Met WikiLeaks*. New York - London: OR Books.

Assange, J. *et al.* (2012). *Cypherpunks: Freedom and the Future of the Intenet*. New York - London: OR Books.

Asur, S., Huberman, B.A., Szabo, G. y Wang, C. (2011). *Trends in Social Media: Persistence and Decay*. Palo Alto, California: HP Lab.

Bách khoa toàn thư trực tuyến về bí mật của các chính phủ. (2007, 24 de enero). *Dantri*. Disponible en: <http://dantri.com.vn/the-gioi/bach-khoa-toan-thu-truc-tuyen-ve-bi-mat-cua-cac-chinh-phu-1169707029.htm> [Consulta: 16 de abril de 2014].

Ball, J. (2011, 2 de septiembre). WikiLeaks publishes full cache of unredacted cables. *The Guardian*. Disponible en: <http://www.theguardian.com/media/2011/sep/02/wikileaks-publishes-cache-unredacted-cables>. [Consulta: 28 de mayo de 2014].

Ball, J. (2012, 27 de febrero). WikiLeaks publishes Stratfor emails linked to Anonymous attack. *The Guardian*. Disponible en: <http://www.theguardian.com/media/2012/feb/27/wikileaks-publishes-stratfor-emails-anonymous>. [Consulta: 4 de junio de 2013].

Ball, J., Schneier, B. y Greenwald, G. (2013, 4 de octubre). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*. Disponible en: <http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption> [Consulta: 18 de diciembre de 2013].

Bandari, R., Asur, S., Huberman, B.A. (2012). The pulse of news in social media: Forecasting popularity. En *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* (pp. 26-33). Palo Alto, California: AAAI Press

Barbrook, R. (2002). *The Regulation of Liberty: Free Speech, Free Trade and Free Gifts on the Internet. Science as Culture*. Vol. 11, 2, pp. 155-170.

Barkham, P. (2011, 1 de marzo). Why is Julian Assange trademarking his name? *The Guardian*. Disponible en: <http://www.theguardian.com/media/2011/mar/01/why-julian-assange-trademarking-name> [Consulta: 5 de diciembre de 2011].

Barlow, J.P. (1990, 8 de junio). *Crime and Puzzlement*. Electronic Frontier Foundation. Disponible en: <https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html> [Consulta: 1 de abril de 2014].

Barlow, J.P. (1996, 8 de febrero). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. Disponible en: <https://projects.eff.org/~barlow/Declaration-Final.html> [Consulta: 1 de abril de 2014].

Barok, D. (2011, 19 de mayo). *Sourced in, unsourced out: Leaking as the common knowledge production*. Master Media Design and Communication: Networked Media. Piet Zwart Institute, Rotterdam.

Barthes, R. (1966). Introduction à l'analyse structurale des récits. *Communications*, 8(1), pp. 1-27.

Bassett, E.H. y O'Riordan, K. (2002). Ethics of Internet research: Contesting the human subjects research model. *Ethics and Information Technology*, 4(3), pp. 233-247.

Baudrillard, J. (1981). Requiem for the media. En Wardrip-Fruin, N y Montfort, N (eds.) (2003), *The New Media Reader* (pp. 278-288). Cambridge: MIT Press.

Baudrillard, J. (1985). El éxtasis de la comunicación. En Foster, Hal (ed.) (1986), *La Postmodernidad* (pp. 187-198). Barcelona: Kairós.

Baudrillard, J. (1987). *The Ecstasy of Communication*. New York: Semiotext(e).

Baudrillard, J. (1988). *El otro por sí mismo*. Barcelona: Anagrama.

Baudrillard, J. (1991). *La transparencia del mal. Ensayo sobre los fenómenos extremos*. Barcelona: Anagrama.

Bauman, Z. (2003). *Modernidad Líquida.* México: Fondo de Cultura Económica.

Bauman, Z. (2007). *Tiempos Líquidos. Vivir en una época de incertidumbre*. Barcelona: Tusquets Editores.

BBC. (2012, 1 de mayo). *Anonymous 'hacktivist' goes public on cyber protests* [archivo de vídeo]. Disponible en: <http://www.bbc.com/news/magazine-17914501> [Consulta: 16 de febrero de 2014].

Becker, H.S. y Geer, B. (1958). Participant observation and interviewing: a rejoinder. *Human Organization*, vol. 17, nº. 2, pp. 39-40.

Beeler, M., Gosper, R.W. y Schroeppel R. (1972, 29 de febrero). *HAKMEM*. Artificial Intelligence Memo, nº 239. Massachusetts Institute of Technology A. I. Laboratory. Disponible en: <http://www.inwap.com/pdp10/hbaker/hakmem/hakmem.html> [Consulta: 8 de febrero de 2014].

Bell, D. (1973). *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York: Basic Books.

Bell, G. B. (2011). Digital Whistleblowing in Restricted Environments. *Journal of Digital Information*, vol. 12 , nº 3.

Bendyka, E. (2007, 13 de enero). WikiLeaks - bat na dyktaturę. *Polityka*. Disponible en: <http://bendyk.blog.polityka.pl/2007/01/13/wikileaks-bat-na-dyktature/> [Consulta: 17 de abril de 2014].

Bernstein, M., Bakshy, E., Burke, M. y Karrer, B. (2013). Quantifying the Invisible Audience in Social Networks. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 21-30). New York: ACM Press.

Best, K. (2003). The Hacker's Challenge: Active Access to Information, Visceral Democracy, and Discursive Practice. *Social Semiotics*, (13)3, pp. 263-282.

Bey, H. (1991). *T. A. Z. The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. New York: Autonomedia.

Billhard, S. (2007, 17 de enero). Webseite für Staatsgeheimnisse. *Focus*. Disponible en: <http://www.focus.de/digital/internet/wikileaks_aid_122861.html> [Consulta: 17 de abril de 2014].

Bilton, N. (2011, 28 de agosto). Twitter Becomes a Playground During Hurricane Irene. *The New York Times*. Disponible en: <http://bits.blogs.nytimes.com/2011/08/28/twitter-becomes-adult-playground-during-hurricane-irene/> [Consulta: 15 de febrero de 2013].

Blaikie, Norman W.H. (1991). A critique of the use of triangulation in social research. *Quality and Quantity*, nº 25, pp. 115-136.

Blakely, R. (2007, 27 de enero). The week on the web: The truth is out there… maybe. *The Times*. Disponible en: <http://www.thetimes.co.uk/tto/technology/internet/article1860548.ece> [Consulta: 16 de abril de 2014].

Bleikelia, M. (2007, 15 de enero). Legger ut hemmelige dokumenter på nett. *VG*. Disponible en: <http://www.vg.no/forbruker/teknologi/data-og-nett/legger-ut-hemmelige-dokumenter-paa-nett/a/178575/> [Consulta: 17 de abril de 2014].

Borsook, P. (2001). *Cyberselfish: A Critical Romp through the Terribly Libertarian Culture of High Tech*. New York: Public Affairs.

Boushka, B. (2007, 15 de enero). Wikileaks is a new tool for anonymous dissent. *Bill on International Issues*. Disponible en: <http://billboushkaint.blogspot.com/2007/01/wikileaks-is-new-tool-for-anonymous.html> [Consulta: 18 de abril de 2014].

Boyd, D. y Crawford, K. (2012). Critical Questions For Big Data. *Information, Communication & Society*, 15(5), pp. 662-679.

Bradner, S. (2007, 17 de enero). Wikileaks: a site for exposure. *Network World*. Disponible en: <http://www.networkworld.com/article/2302997/infrastructure-management/bradner--wikileaks--a-site-for-exposure.html> [Consulta: 15 de abril de 2014].

Bradley Manning's Excessive Sentence (2013, 21 de agosto). *The New York Times*. Disponible en: <http://www.nytimes.com/2013/08/22/opinion/bradley-mannings-sentence-is-excessive.html> [Consulta: 13 de diciembre de 2013].

Braman, S. (2014). "We Are Bradley Manning": Information Policy, the Legal Subject, and the WikiLeaks Complex. *International Journal of Communication*, 8, pp. 2603–2618.

Brand, S. (1987): *The Media Lab: inventing the future at MIT*. New York: Viking.

Brown, P., Lauder, H. y Ashton, D. (2011). *The Global Auction: The Broken Promises of Education, Jobs, and Incomes*. Oxford: Oxford University Press.

Bruns, A. (2014). WikiLeaks: The Napster of Secrets? *International Journal of Communication*, 8, pp. 2646–2651.

Butcher, S. (2011, 12 de febrero). Assange helped our police catch child pornographers. *The Age*. Disponible en: <http://www.theage.com.au/victoria/assange-helped-our-police-catch-child-pornographers-20110211-1aqnl.html> [Consulta: 8 de octubre de 2015].

Cardeñosa, B. (2011). *W de WikiLeaks. La venganza contra las mentiras del poder*. Barcelona: Libros Cúpula.

Careaga Mercadillo, A.L. (2010): *Wikis: Las comunidades del conocimiento*. Instituto Tecnológico de Teléfonos de México S.C.

Carr, D. (2011a, 5 de noviembre). Is this the WikiEnd? *The New York Times*. Disponible en: <http://www.nytimes.com/2011/11/06/sunday-review/is-the-wikileaks-movement-fading.html> [Consulta: 8 de diciembre de 2011].

Carr, D. (2011b, 11 de diciembre). When Truth Survives Free Speech. *The New York Times*. Disponible en: <http://www.nytimes.com/2011/12/12/business/media/when-truth-survives-free-speech.html> [Consulta: 15 de febrero de 2013].

Carr, N. (2006, 19 de diciembre). Sharecropping the Long Tail. *Rough Type*. Disponible en: <http://www.roughtype.com/archives/2006/12/sharecropping_t.php> [Consulta: 10 de enero de 2013].

Carr, R. (2007, 22 de enero). Cyber leakers now have a place to go; Web site says goal is better government. *The Atlanta Journal-Constitution*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Carvajal Prieto, M., García Avilés, J.A. y González Esteban, J.L. (2011). The News Production Process about the U.S. Embassy Cables: How 'The Guardian', 'The New York Times' and 'El País' Covered and Released the Documents Provided by WikiLeaks (pp. 83-91). En Salaverría, R (ed.), *Diversity of Journalisms. Proceedings of the ECREA Journalism Studies Section and 26th International Conference of Communication (CICOM)* at University of Navarra, Pamplona, 4-5 July 2011. Pamplona: Servicio de Publicaciones de la Universidad de Navarra.

Castells, M. (1997). *La era de la información: economía, sociedad y cultura. Vol. 1. La sociedad red*. Madrid: Alianza Editorial.

Castells, M. (2001a). *La Galaxia Internet*. Barcelona: Plaza & Janés.

Castells, M. (2001b). Informationalism and the Network Society. En Pekka Himanen, *The Hacker Ethic and the Spirit of Information Age* (pp. 155-178). New York: Random House.

Castells, M. (2006). *La Sociedad Red: una visión global*. Madrid: Alianza Editorial.

Castells, M. (2009). *Comunicación y poder*. Madrid: Alianza Editorial.

Castells, M., Fernández-Ardévol, M., Linchaun Qiu, J. y Sey, A. (2007). *Comunicación móvil y sociedad. Una perspectiva global*. Barcelona: Ariel-Fundación Telefónica.

CBC News. (2010, 1 de diciembre). *Flanagan regrets WikiLeaks assassination remark*. Disponible en: <http://www.cbc.ca/news/politics/flanagan-regrets-wikileaks-assassination-remark-1.877548> [Consulta: 18 de diciembre de 2011].

Ceberio Belaza, M., Doncel, L., Irujo, J. y Peregil, F. (2011, 25 de abril). Los abusos de Guantánamo, al descubierto. *El País*. Disponible en: <http://www.elpais.com/articulo/internacional/abusos/Guantanamo/descubierto/elpepuint/20110425elpepuint_4/Tes> [Consulta: 12 de diciembre de 2011].

Chadwick, A. (2011). *The Hybrid Media System: Politics & Power*. Oxford: Oxford University Press.

Chamberlain, P.R. (2010). Twitter as a Vector for Disinformation. *Journal of Information Warfare* 9(1), pp. 11-17. School of Computer & Security Science, Edith Cowan University, Australia.

Chatfield, T. (2014, 18 de noviembre). *Apple's fashionable seduction.* BBC Future. Disponible en: <http://www.bbc.com/future/story/20121026-apples-fashionable-seduction> [Consulta: 8 de junio de 2015].

Chelsea Manning Support Network. (2013, 25 de julio). *We Are Bradley Manning* [campaña publicitaria]. En *The New York Times*, p. A15.

Chelsea Manning Support Network (s.f). *About Chelsea Manning*. Disponible en <http://www.chelseamanning.org/learn-more/bradley-manning>. [Consulta: 14 de diciembre de 2013].

Christensen, Ch. y Jónsdóttir, B. (2014). WikiLeaks, Transparency, and Privacy: A Discussion with Birgitta Jónsdóttir. *International Journal of Communication*, 8, pp. 2558-2566.

ChurchOfScientology (2008, 21 de enero). *Message to Scientology* [archivo de vídeo]. Disponible en: <https://youtu.be/JCbKv9yiLiQ> (última consulta: 19 de mayo de 2014).

ChurchOfScientology (2008, 27 de enero). *Call to Action* [archivo de vídeo]. Disponible en: <https://youtu.be/YrkchXCzY70> (última consulta: 19 de mayo de 2014).

ChurchOfScientology (2008, 1 de febrero). *Code of Conduct* [archivo de vídeo]. Disponible en: <https://youtu.be/-063clxiB8I> [Consulta: 19 de mayo de 2014].

Cilenis Language Technology (2014). Linguakit [suite de herramientas lingüísticas]. Disponible en: <https://linguakit.com>

Ciszewski, B. (2007, 18 de enero). Powstaje internetowa platforma dla dysydentów. *Money.pl*. Disponible en: <http://www.money.pl/gospodarka/polityka/artykul/powstaje;internetowa;platforma;dla;dysydentow,104,0,216680.html> [Consulta: 17 de abril de 2014].

Clarke, I. (1999). *A Distributed, Decentralised Information Storage and Retrieval System*. Edinburgh: Division of Informatics, University of Edinburgh.

Clarke, R. (1999). *Information Wants To Be Free…* Xamax Consultancy Pty Ltd. Disponible en: <http://www.rogerclarke.com/II/IWtbF.html>. [Consulta: 22 de enero de 2014].

Clinton, B. (1999, 22 de enero). *Remarks by the President on 'Keeping America Secure for the 21st Century'*. National Academy of Sciences, Washington DC, vol. 96, pp. 3486-3488. Disponible en: <http://www.pnas.org/content/96/7/3486.full.pdf> [Consulta: 16 de julio de 2014].

Cohen, B. (1963). *The press and foreign policy*. Princeton: Princeton University Press.

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London - New York: Verso.

Coleman, G. y Golub, A. (2008). Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism. *Anthropological Theory*, 8(3), pp. 255-277.

Condon, S. (2010, 29 de noviembre). *Congress Lashes Out at Wikileaks, Senators Say Leakers May Have "Blood on their Hands"*. CBS News. Dispobible en: <http://www.cbsnews.com/news/congress-lashes-out-at-wikileaks-senators-say-leakers-may-have-blood-on-their-hands/> [Consulta: 15 de diciembre de 2011].

Conover M.D., Davis C., Ferrara E., McKelvey K., Menczer F. y Flammini A. (2013). The Geospatial Characteristics of a Social Movement Communication Network. *PLOS ONE* 8(3): e55957.

Conover M.D., Ferrara E., Menczer F. y Flammini A. (2013). The Digital Evolution of Occupy Wall Street. *PLoS ONE* 8(5), e64679.

Costanza-Chock S. y Rey-Mazón, P. (in press). PageOneX: New Approaches to Newspaper Front Page Analysis. *International Journal of Communication*.

Cook, T.D. y Reichardt, Ch.S. (1986). *Métodos cualitativos y cuantitativos en investigación evaluativa*. Madrid: Ediciones Morata.

Coupland, D. (1994, 1 de enero). Microserfs. *Wired*. Disponible en: <http://www.wired.com/1994/01/microserfs/> [Consulta: 13 de noviembre de 2013]

Coupland, D. (1995). *Microserfs*. New York: HarperCollins.

Crispin, M. (1978). *Software Wars*. Disponible en: <http://www.inwap.com/pdp10/software-wars.txt> [Consulta: 9 de junio de 2014].

Critical Art Ensemble (1994). *The Electronic Disturbance*. New York: Autonomedia.

Critical Art Ensemble (1996). *Electronic Civil Disobedience and Other Unpopular Ideas*. New York: Autonomedia.

Cult of the Dead Cow (2004, 31 de julio). *About - Who We Be*. Disponible en: <http://w3.cultdeadcow.com/cms/about.html> [Consulta: 18 de marzo de 2014].

Cult of the Dead Cow (2001). *The Hacktivismo FAQ v1.0*. Disponible en: <http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html> [Consulta: 18 de marzo de 2014].

Czepeck, A. (2011). Getting Personal: Personification vs. Data-Journalism as an International Trend in Reporting about Wikileaks. En Salaverría, R. (ed.), *Diversity of Journalisms. Proceedings of the ECREA Journalism Studies Section and 26th International Conference of Communication (CICOM)* at University of Navarra, Pamplona, 4-5 July 2011. Pamplona: Servicio de Publicaciones de la Universidad de Navarra, pp. 94-108.

Daley, B. (2007, 4 de enero). Leaks Go Wiki. *Project On Government Oversight Blog*. Disponible en: <http://pogoblog.typepad.com/pogo/2007/01/leaks_go_wiki.html> [Consulta: 15 de abril de 2014].

Daly, A. (2014). Internet Privatization, WikiLeaks, and Free Expression. *International Journal of Communication*, 8, 2693–2703.

Dann, J. y Dozois, G. (eds.). (1996). *Hackers*. New York: Ace Books.

DeAngelis, S. (2014, 24 de enero). Wikileaks and Secrecy. *Enterra Insights*. Disponible en: <http://enterpriseresilienceblog.typepad.com/enterprise_resilience_man/2007/01/wikileaks_and_s.html> [Consulta: 17 de abril de 2014].

Deleuze, G. y Guattari, F. (1987). *A Thousand Plateaus*. Minneapolis: University of Minnesota Press.

Delio, M. (2003, 22 de julio). Hackers Lose a Patron Saint. *Wired*. Disponible en: <http://www.wired.com/science/discoveries/news/2003/07/59711> [Consulta: 9 de diciembre de 2011].

Democracy Now! (2011, 5 de julio). *Full Video of WikiLeaks' Julian Assange & Philosopher Slavoj Žižek With Amy Goodman* [archivo de vídeo]. Disponible en: <http://www.democracynow.org/blog/2011/7/5/watch_full_video_of_wikileaks_julian_assange_philosopher_slavoj_iek_with_amy_goodman> [Consulta: 1 de diciembre de 2011].

Denning, D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. En Arquila, J. y Ronfelt, D. (eds.), *Networks and Netwars: The Future of Terror, Crime and Militancy* (pp. 239-288). Santa Mónica, California: RAND Corporation.

Denzin, N.K. (1970). *Sociological Methods: a Source Book*. Chicago: Aldine Publishing Company.

Dersjant, Th. (2007, 14 de enero). Wikileaks: internetloket voor klokkenluiders. De *Nieuwe Reporter*. Disponible en: <http://www.denieuwereporter.nl/2007/01/wikileaks-internetloket-voor-klokkenluiders/> [Consulta: 17 de abril de 2004].

Dias Souza, M. (2011). *Jornalismo e Cultura da Convergência: A Narrativa Transmídia na Cobertura do Cablegate nos Sites El País e Guardian*. Universidade Federal de Santa Maria. Centro de Ciências Sociais e Humanas. Departamento de Ciências da Comunicação. Programa de Pós-Graduação em Comunicação. Mestrado em Comunicação Midiática.

Díaz, S. y Lozano, J. (eds.). (2013). *Vigilados: WikiLeaks o las nuevas fronteras de la información*. Madrid: Biblioteca Nueva.

Dissidents take whistle-blowing global with leaking Web site. (2007, 17 de enero). *Victoria Advocate*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Domscheit-Berg, D. (2011). *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo*. Barcelona: Roca Editorial.

DonSaeid (2007, 23 de enero). اسناد ه هلرحم در ت نرتنن يلي *Tapesh.com*. Disponible en: <https://wikileaks.org/wiki/Media/اسناد_ه هلرحم_در_ت نرتنن يلي> [Consulta: 16 de abril de 2014].

Dreyfus, S. y Assange, J. (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Kew (Australia): Mandarin.

Echevarría, B. (2011, 16 de octubre). "Comunicar es el nuevo entretenimiento de la gente". *El País*. Disponible en: <http://elpais.com/diario/2011/10/16/radiotv/1318716001_850215.html> [Consulta: 13 de febrero de 2013].

Eisner, E.W. (1977). Critique. *Anthropology and Education Quarterly*. 8: 71-72.

El Akkad, O. (2010, 5 de diciembre). U.S. government powerless to plug WikiLeaks. *The Globe and Mail*. Disponible en: <http://www.theglobeandmail.com/news/technology/us-government-powerless-to-plug-wikileaks/article1825962/> [Consulta: 12 de diciembre de 2012].

Electronic Disturbance Theater (1998a, 1 de enero). *Intercontinental Cyberspace Liberation Army Declares Netwar Against the Mexican State*. Disponible en: <http://www.thing.net/~rdom/ecd/hoax.html> [Consulta: 30 de septiembre de 2014].

Electronic Disturbance Theater (1998b, 10 de septiembre). *Chronology of SWARM*. Disponible en: <http://www.thing.net/~rdom/ecd/CHRON.html> [Consulta: 30 de septiembre de 2014].

Electronic Frontier Foundation (1990, 1 de marzo). *Steve Jackson Games v. Secret Service Case Archive*. Disponible en: <https://w2.eff.org/legal/cases/SJG/> [Consulta: 4 de abril de 2014].

Electronic Privacy Information Center. (s.f.). *The 2600 Case*. Disponible en: <https://epic.org/security/2600/> y <https://epic.org/security/hackers/2600/> [Consulta: 14 de junio de 2014].

Elías, C. (2003). Adaptación de la metodología de "observación participante" al estudio de los gabinetes de prensa como fuentes periodísticas. *Empiria. Revista de Metodología de Ciencias Sociales*, Nº 6, pp. 145-159.

Elías, C. (2011). ¿Wikileaks es periodismo ciudadano? De la ética hacker del Cablegate a la estética emo de Assange como icono global. *Actas del III Congreso Internacional Latina de Comunicación Social*. Universidad de La Laguna, diciembre.

Elías, C. (2015a). *El selfie de Galileo. Software social, político e intelectual del siglo XXI*. Barcelona: Península-Planeta.

Elías, C. (2015b). *Big data y periodismo en la sociedad red*. Madrid: Síntesis.

Elola, J. (2010, 24 de octubre). Cita secreta con el hombre que hace temblar al Pentágono. *El País*. Disponible en: <http://www.elpais.com/articulo/reportajes/Cita/secreta/hombre/hace/temblar/Pentagono/elpepusocdmg/20101024elpdmgrep_1/Tes> [Consulta: 28 de noviembre de 2011].

Emmett, L. (2011, 2 de mayo). *WikiLeaks revelations only tip of iceberg – Assange* [archivo de vídeo]. RT. Disponible en: <http://rt.com/news/wikileaks-revelations-assange-interview/> [Consulta: 2 de diciembre de 2011].

Enyon, R., Schroeder, R. y Fry, J. (2009). New techniques in online research: Challenges for research ethics. *Twenty First Century Society*, 4(2), pp. 187-199.

Enzensberger, H.M. (1970). Constituents of a Theory of the Media. En Wardrip-Fruin, N. y Nick Montfort (eds.) (2003), *The New Media Reader* (pp. 261-275). Cambridge: MIT Press.

Epstein, J. (2010, 29 de noviembre). King: Prosecute WikiLeaks, Assange. Politico. Disponible en: <http://www.politico.com/story/2010/11/king-prosecute-wikileaks-assange-045667> [Consulta: 16 de diciembre de 2011].

Estulin, D. (2011). *Desmontando WikiLeaks*. Barcelona: Ediciones del Bronce.

Eurinomo y Quickzero (2008, 4 de noviembre). The Portuguese Scene. *Phrack Magazine*. Disponible en: <http://phrack.org/issues/65/15.html> [Consulta: 10 de julio de 2014].

Featherstone, M. (1988). In Pursuit of the Postmodern: An Introduction. *Theory, Culture and Society*, 5, 2-3, pp. 195-215.

Fernández Chico, J.M. (2011). Los tres derrumbes y la nueva configuración geopolítica de la seguridad en Internet. La caída del muro de Berlín, el 11/9 y Wikileaks. *Razón y Palabra*, vol. 16, nº 75.

Forbes, P. (director). (2011). *WikiLeaks: Secrets and Lies* [documental]. Reino Unido: Oxford Film and Television.

Franck, G. (1999, 7 de diciembre). The Economy of Attention. *Telepolis*. Disponible en: <http://www.heise.de/tp/artikel/5/5567/1.html> [Consulta: 18 de enero de 2013].

Freedman, D. y Mann, C. (1997). *At Large: The Strange Case of the World's Biggest Internet Invasion*. New York: Simon and Schuster.

Friedman, D. (2007, 4 de enero). Web site aims to post government secrets. *Federal Times*. Disponible en: <http://cryptome.org/wikileaks/wikileaks-leak.htm> [Consulta: 14 de abril de 2014].

Frantzell, L. (2007, 23 de enero). WikiLeaks.org: en wiki för hemliga dokument. *Det Progressiva USA*. Disponible en: <http://www.usabloggen.se/2007/01/23/wikileaksorg-en-wiki-for-hemliga-dokument/> [Consulta: 16 de abril de 2014].

Free Software Foundation (2007, 29 de junio). *GNU General Public License v3.0*. Disponible en: <http://www.gnu.org/licenses/gpl-3.0.en.html> [Consulta: 16 de marzo de 2014].

Friedman, M. (2010, 13 de diciembre). Julian Assange: Readers' Choice for TIME's Person of the Year 2010. *Time*. Disponible en: <http://newsfeed.time.com/2010/12/13/julian-assange-readers-choice-for-times-person-of-the-year-2010/> [Consulta: 11 de diciembre de 2011].

Foucault, M. (1975). *Vigilar y Castigar. El nacimiento de la pri*sión. Madrid: Siglo XXI Editores, 2008.

Foucault, M. (2003). *La verdad y las formas jurídicas*. Barcelona: Gedisa.

Fowler, A. (2011). *The Most Dangerous Man in the World: The Explosive True Story of Julian Assange and the Lies, Cover-ups and Conspiracies He Exposed*. New York: Skyhorse Publishing.

Fuchs, Ch. (2014). WikiLeaks and the Critique of the Political Economy. *International Journal of Communication*, 8, 2718–2732.

Gamallo, P. (2016). Herramienta 1 con aplicación en el aula: Linguakit. En Mª José Domínguez y Mª Teresa Sanmarco (eds.), *Lexicografía y didáctica de lenguas*. Frankfurt: Peter Lang.

Gans, H.J. (2003). *Democracy and the News*. New York: Oxford University Press.

Gallego Aguilar, A.F. (2011). *Diseño de narrativas transmediáticas*. Manizales, Colombia: Universidad de Caldas, Facultad de Artes y Humanidades. Maestría en Diseño y Creación Interactiva.

Gergen, K.J. (1992). *El yo saturado. Dilemas de la identidad en el mundo contemporáneo*. Barcelona: Paidós.

Giles, J. (2005). Internet encyclopaedias go head to head. *Nature*, 438 (7070), pp. 900-901.

Gilboa, N. (2001, 1 de febrero). Getting Gray With The Internet Liberation Front. Disponible en: <http://www.grayarea.com/ilf7.htm> [Consulta: 13 de septiembre de 2014].

Gilson, D. (2007, 4 de enero). Whistleblowers Get Their Own Wikipedia. *Mother Jones*. Disponible en: <http://www.motherjones.com/mojo/2007/01/whistleblowers-get-their-own-wikipedia> [Consulta: 17 de abril de 2014].

Glasscastle (2007, 11 de enero). Opening Up the Rabbit Hole. *Harvard's Dowbrigade Blog*. Disponible en: <http://blogs.law.harvard.edu/dowbrigade/2007/01/11/opening-up-the-rabbit-hole/> [Consulta: 17 de abril de 2014].

Glave, J. (1998, 3 de julio): *Anti-Nuke Cracker Strikes Again*. Wired. Disponible en: <http://archive.wired.com/science/discoveries/news/1998/07/13446> [Consulta: 23 de septiembre de 2015].

Gnome's Lair y Kyratzes, J. (2011). *WikiLeaks Stories*. Disponible en <http://wikileaks-stories.com/> y <https://wikileaksstories.wordpress.com/> [Consulta: 30 de noviembre de 2011].

Goldstein, E. (director). (2001). *Freedom Downtime* [documental]. Estados Unidos: 2600 Films.

Goldstein, E. (ed.) (2009). *The Best of 2600: A Hacker Odyssey, Collector's Edition*. Indianapolis: Wiley Publishing, Inc.

Gómez Cruz, E. (2002). Espacio, ciberespacio e hiperespacio: nuevas configuraciones para leer la comunicación mediada por computadora. *Anuario de Investigación de la Comunicación CONEICC IX*. México.

Gómez Cruz, E. (2003). *Cibersexo. ¿La última frontera del Eros? Un estudio etnografico*. Colima, México: Universidad de Colima.

González-Bailón, S., Wang, N., Rivero, A., Borge-Holthoefer, J. y Moreno, Y. (2011). Protest Recruitment through an Online Network. *Nature Scientific Reports* 1(197).

Goverup1 (2007, 2007). Tomorrow's Deep Throat: Wikileaks. *Daily Kos*. Disponible en: <http://www.dailykos.com/story/2007/01/14/290634/-Tomorrow-s-Deep-Throat-160-Wikileaks> [Consulta: 17 de abril de 2014].

Graves, S. E.. (2008). Prior Restraint or Finger in the Dike? Bank Julius Baer v. Wikileaks and Dynadot. *The Justice System Journal*, 29(2), 216–219.

Greenberg, A. (2010, 29 de noviembre). An Interview With WikiLeaks' Julian Assange. *Forbes*. Disponible en: <http://www.forbes.com/sites/andygreenberg/2010/11/29/an-interview-with-wikileaks-julian-assange/> [Consulta: 8 de julio de 2014].

Greenwald, G. (2010, 15 de diciembre). The inhumane conditions of Bradley Manning's detention. *Salon*. Disponible en: <http://www.salon.com/2010/12/15/manning_3/>. [Consulta: 12 de diciembre de 2013).

Grossman, L. (2010, 15 de diciembre). Person of the Year: Mark Zuckerberg. *Time*. Disponible en: <http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183,00.html> [Consulta: 11 de diciembre de 2011].

Guardian journalist negligently disclosed Cablegate passwords (2011, 1 de septiembre). *The Guardian*. Disponible en: <https://wikileaks.org/Guardian-journalist-negligently.html> [Consulta: 28 de mayo de 2014].

Gutiérrez-Rubí, A. (2011). Del storytelling al microblogging. *Cuadernos de Comunicación Evoca, 4 (Comunicación política 2.0),* pp. 17-21.

Haberman, H. (2007, 4 de enero). Wikileaks Site Will Offer Safe Harbor For Whistle Blowers. *Dungeon Diary*. Disponible en: <https://wikileaks.org/wiki/Media/Wikileaks_Site_Will_Offer_Safe_Harbor_For_Whistle_Blowers> [Consulta: 16 de abril de 2014].

Hacktivismo. (2004). *About Hacktivismo* (2004). Disponible en: <http://www.hacktivismo.com/about/index.php> [Consulta: 26 de marzo de 2014].

Hacktivismo y Cult of the Dead Cow (2001, 4 de julio). *La Declaración del Hacktivismo*. Disponible en: <http://www.hacktivismo.com/public/declarations/es.php> [Consulta: 26 de abril de 2014].

Hafner, K. y Markoff, J. (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.

Hafner K. y Lyon, M. (1996). *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon & Schuster.

Hannemyr, G. (1999, 1 de febrero). Technology and pleasure: Considering hacking constructive. *First Monday*, vol. 4, nº 2. Disponible en: <http://firstmonday.org/ojs/index.php/fm/article/view/647/562> [Consulta: 19 de junio de 2014].

Harmon, A. (1998a, 14 de septiembre). Hacker Group Commandeers The New York Times Web Site. *The New York Times*. Disponible en: <http://www.nytimes.com/1998/09/14/us/hacker-group-commandeers-the-new-york-times-web-site.html> [Consulta: 24 de septiembre de 2014].

Harmon, A. (1998b, 31 de octubre): 'Hacktivists' of All Persuasions Take Their Struggle to the Web. *The New York Times*. Disponible en: <http://www.nytimes.com/1998/10/31/world/hacktivists-of-all-persuasions-take-their-struggle-to-the-web.html> [Consultado el 24 de septiembre de 2014].

Hastings, M. (2012). Julian Assange: la historia más fascinante del siglo XXI. *Rolling Stone España*, nº148, pp. 44-53.

Hawn, M. (1996, 15 de julio). Fear of a Hack Planet: The Strange Metamorphosis of the Computer Hacker. *The Site*. En Jordan, T. y Taylor, P. (2004), *Hacktivism and Cyberwars: Rebels with a cause?* New York - London: Routledge.

Himanen, P. (2001). *The Hacker Ethic and the Spirit of Information Age*. New York: Random House.

Hoffman, A., Bell, A. y Edison, T. (2010). *Hacking Ma Bell: The First Hacker Newsletter - Youth International Party Line, the First Three Years*. Salt Lake City: Warcry Communications.

Hollinger, R. y Lanza-Kaduce, L. (1988). The Process of Criminalization: The Case of Computer Crime Laws. *Criminology*, vol. 26, pp. 101-126.

Honderich, T. (1995). *Hierarchic Democracy and the Necessity of Mass Civil Disobedience*. London: South Place Ethical Society.

Hood, C. (2011). From FOI World to WikiLeaks World: A New Chapter in the Transparency Story? *Governance*, vol. 24, nº. 4, pp. 635-638.

Houellebecq, M. (2000). *El mundo como supermercado*. Barcelona: Anagrama.

Howe, K.R. (1988). Against Quantitative-Qualitative Incompatibility Thesis or Dogmas Die Hard. *Educational Researcher*, 17(8), pp. 10-16.

Huschle, B.J. (2002). Cyber Disobedience: When is Hacktivism Civil Disobedience? *International Journal of Applied Philosophy*, 16 (l), pp. 69-83.

Holmström, L. (2007, 7 de enero). Gatekeeping is over. *Citizen Media Watch*. Disponible en: <https://wikileaks.org/wiki/Media/Gatekeeping_is_over> y <http://lottaholmstrom.se/2007/01/07/gatekeeping-is-over-new-wiki-enables-anonymous-leaks/> [Consulta: 16 de abril de 2014].

Hosenball, M. (2010, 13 de diciembre). Julian Assange vs The World. *Reuters*. Disponible en: <http://www.reuters.com/article/2010/12/13/us-wikileaks-assange-idUSTRE6BB1LG20101213> [Consulta: 28 de noviembre de 2011].

Hughes, E. (1993, 9 de marzo). *A Cypherpunk's Manifesto*. Disponible en: <http://www.activism.net/cypherpunk/manifesto.html> [Consulta: 28 de noviembre de 2011].

Hughes, S.A. (2011, 26 de agosto). Hurricane Irene: 'Photo' of shark swimming in street is fake. *The Washington Post*. Disponible en: <https://www.washingtonpost.com/blogs/blogpost/post/hurricane-irene-photo-of-shark-swimming-in-street-is-fake/2011/08/26/gIQABHAvfJ_blog.html> [Consulta: 15 de febrero de 2013].

Hush Hush Wikipedia (2007, 11 de enero). *Canberra Times*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Ibáñez, J. (1988). *Cuantitativo/Cualitativo*. En Reyes R.: *Terminología Científico-Social*. Barcelona: Anthropos.

Igartua, J. J. y Humanes, M. L. (2004). *El método científico aplicado a la investigación en comunicación social*. Portal de la Comunicación InCom-UAB. Aula abierta.

Intercontinental Conference on Alternative Use of Technology Amsterdam (1989, agosto). *ICATA '89 Declaration*. Disponible en <http://www.lucsala.nl/myster/school/icata89.html>[Consulta: 8 de julio de 2014].

Ipsos (2011, 26 de abril). *Ipsos Global @dvisory: Julian Assange and WikiLeaks*. Disponible en: <http://www.ipsos-na.com/download/pr.aspx?id=10833> [Consulta: 12 de diciembre de 2011].

Is Wikileaks A Good Idea? (2007, 7 de enero). *Say Anything*. Disponible en: <https://sayanythingblog.com/entry/is_wikileaks_a_good_idea/> [Consulta: 16 de abril de 2014].

Is WikiLeaks.org the right idea for a whistleblowing website? (2007, 5 de enero). *Spy Blog*. Disponible en: <http://p10.hostingprod.com/@spyblog.org.uk/blog/2007/01/05/is-wikileaksorg-the-right-idea-for-a-whistleblowing-website.html> [Consulta: 16 de abril de 2014].

Isaacson, W. (2011). *Steve Jobs*. Barcelona: Debate.

Iskold, A. (2007, 1 de marzo). The Attention Economy. *ReadWrite*. Disponible en: <http://www.readwriteweb.com/archives/attention_economy_overview.php> [Consulta: 21 de diciembre de 2012].

Jarvis, L., Macdonald, S. y Chen, T. (eds.) (2015). *Terrorism Online: Politics, Law and Technology*. New York - London: Routledge.

Jefferson, T. (1813, 13 de agosto). Thomas Jefferson to Isaac McPherson. En *The Writings of Thomas Jefferson* (1905). Andrew A. Lipscomb y Albert Ellery Bergh (eds.). 20 vols. Washington: Thomas Jefferson Memorial Association.

Jenkins, H. (2008). *Convergence Culture: La cultura de la convergencia de los medios de comunicación*. Barcelona: Ediciones Paidós Ibérica.

Jick, T. D. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in action. *Administrative Science Quarterly*, 24(4), pp. 602-610.

Jiménez, V. y Caño, A. (2010, 28 de noviembre). La mayor filtración de la historia deja al descubierto los secretos de la política exterior de EE UU. *El País*. Disponible en: <http://www.elpais.com/articulo/internacional/mayor/filtracion/historia/deja/descubierto/secretos/politica/exterior/EE/UU/elpepuint/20101128elpepuint_25/Tes> [Consulta: 30 de noviembre de 2011].

Jones, S. y Brown, J.W. (2011). *'The Assange Effect': Wikileaks, the Espionage Act and the Fourth Estate*. *Media Law Resource Center Bulletin*, vol. 2, pp. 115-147.

Jordan, T. (1999). *Cyberpower: the culture and politics of cyberspace and the Internet*. London: Routledge.

Jordan, T. (2002). *Activism!: Direct Action, Hacktivism and the Future of Society*. London: Reaktion Books.

Jordan, T. y Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a cause?* New York - London: Routledge.

Jurgenson, N. y Rey, PJ (2014). Liquid Information Leaks. *International Journal of Communication*, 8, pp. 2651–2665.

Juris, J. (2008). *Networking futures: The movement against corporate globalization*. Durham - London: Duke University Press.

Kane, P. (1989). *V.I.R.U.S. Protection: Vital Information Resources Under Siege*. New York: Bantam.

Karatzogianni, A. y Robinson, A. (2014). Digital Prometheus: WikiLeaks, the State–Network Dichotomy, and the Antinomies of Academic Reason. *International Journal of Communication*, 8, pp. 2704–2717.

Karp, S. (2006, 13 de septiembre). The 2.0 Control Paradox. *Publishing 2.0*. Disponible en: <http://publishing2.com/2006/09/13/the-20-control-paradox/> [Consulta: 12 de diciembre de 2012].

Katz, E. y Lazarsfeld, P.F. (1955). *Personal Influence: The Part Played by People in the Flow of Mass Communications*. Glencoe, Illinois: Free Press.

Keller, B. (2011, 26 de enero). Dealing with Assange and the Wikileaks Secrets. *The New York Times*. Disponible en: <http://www.nytimes.com/2011/01/30/magazine/30Wikileaks-t.html> [Consultado el 7 de diciembre de 2011].

Kelsey, T. (1994, 24 de noviembre). The BT Hacker Scandal: Revealed: How Hacker Penetrated the Heart of British Intelligence. *The Independent*. Disponible en: <http://www.independent.co.uk/news/the-bt-hacker-scandal-revealed-how-hacker-penetrated-the-heart-of-bri-tish-intelligence-1439935.html> [Consulta: 16 de diciembre de 2013].

Keohane, R.O. y Nye, J.S. Jr. (1998). *Power and Interdependence in the Information Age*. Foreign Affairs, vol. 77, nº 5, pp. 81-94.

Knappenberger, B. (director y guionista). (2012). *We Are Legion: The Story of the Hacktivists* [documental]. Estados Unidos: Luminant Media.

Koman, R. (2007, 15 de enero). *Wikileaks gives an online home to repressed dissidents*. *ZDNet Government*. Disponible en: <http://www.zdnet.com/article/wikileaks-gives-an-online-home-to-repressed-dissidents/> [Consulta: 15 de abril de 2014].

Krol, A. (2007, 14 de enero). Wikifuites. *Vigile.Québec*. Disponible en: <https://wikileaks.org/wiki/Media/Wikifuites> [Consulta: 16 de abril de 2014].

Kubieziel, J. (2007, 6 de enero). Dokumente Befreien. *Qbi's Weblog*. Disponible en: <http://www.kubieziel.de/blog/archives/606-Dokumente-befreien.html> [Consulta: 18 de abril de 2014].

Lackner, Ch. (2007, 13 de enero). Wikileaks ready to expose wrongs: Site offers anonymity to whistleblowers. *Edmonton Journal*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Lackner, Ch. (2007, 13 de enero). Tattle in secret on new Web site. *The Leader-Post* . Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Lackner, Ch. (2007, 13 de enero). Website's aim is to protect snitches: Now those who tell tales can do so in safety. *Nanaimo Daily News*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Lackner, Ch. (2007, 13 de enero). Anonymity guaranteed on whistleblower website: Organizers say site will promote government changes; critics warn of credibility challenges. *Times Colonist*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Lackner, Ch. (2007, 13 de enero). Website aims to protect identity of whistleblowers. *Windsor Star*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Lackner, Ch. (2007, 13 de enero). Website aimed at providing forum for anonymous whistleblowers. *The Vancouver Sun*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Landreani, N.F. (1990). Métodos cuantitativos versus métodos cualitativos: un falso dilema. *Ciencia, Docencia y Tecnología*, nº 1, año I, marzo.

Largen, S. (2007, 19 de enero). Site to serve as source for leaks. *The Daily Tar Heel*, University of North Carolina. Disponible en: <https://wikileaks.org/wiki/Media/Site_to_serve_as_source_for_leaks> [Consulta: 16 de abril de 2014].

Lazarsfeld, P.F. y Merton, R.K. (1948). Mass Communication, Popular Taste and Organized Social Action. En L. Bryson (ed.), The *Communication of Ideas* (pp. 95-118). New York: Harper and Row.

Lazer, D. *et al.* (2009). Computational Social Science. *Science*, vol. 323, pp. 721-723.

Leigh, D. (2010, 30 de julio). WikiLeaks 'has blood on its hands' over Afghan war logs, claim US officials. *The Guardian*. Disponible en: <http://www.theguardian.com/world/2010/jul/30/us-military-wikileaks-afghanistan-war-logs> [Consulta: 17 de diciembre de 2011].

Leigh, D. (2015, 29 de noviembre). La era de las filtraciones. *El País*. Disponible en: <http://internacional.elpais.com/internacional/2015/11/26/actualidad/1448548222_604295.html> [Consulta: 29 de noviembre de 2015].

Leigh, D. y Harding, L. (2011). *WikiLeaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia*. Barcelona: Deusto.

Lennon, R. (2010). *Case study of the Wikileaks Whistleblower*. Dublin City University.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. New York: Anchor Press/Doubleday.

Light, R. (1979). *Integrating multiple empirical studies*. Presentado en el congreso anual de la American Educational Research Association, San Francisco.

Lindgren, S. y Lundström, R. (2011). Pirate Culture and Hacktivist Mobilization: The cultural and social protocols of #WikiLeaks on Twitter. *New Media and Society*, vol. 13, nº 6, pp. 999-1018.

Lipovetsky, G. (2006). *Los tiempos hipermodernos*. Barcelona: Editorial Anagrama.

Lippmann, W. (1922): *La opinión pública*. Madrid: Langre, 2003.

Lo Dico, J. (2011, 23 de septiembre). Julian Assange's life story is riding for a spectacular fall. *London Evening Standard*. Disponible en: <http://www.thisislondon.co.uk/standard/article-23990350-julian-assanges-life-story-is-riding-for-a-spectacular-fall.do> [Consultado el 28 de noviembre de 2011].

Lockwood, L. (2007, 12 de enero). Listen Up, Whistleblowers! *Dayly Kos*. Disponible en: <http://www.dailykos.com/story/2007/01/12/290071/-Listen-Up-Whistleblowers> [Consulta: 17 de abril de 2014].

Logan , R. (2011, 12 de abril). Bradley Manning, otra piedra en el zapato de Obama. *BBC*. Disponible en: <http://www.bbc.com/mundo/noticias/2011/04/110412_wikileaks_manning_detenido_sao2.shtml> [Consultado el 28 de noviembre de 2011].

López García, X., Toural Bran, C. y Rodríguez Vázquez, A. (2016). Software, estadística y gestión de bases de datos en el perfil del periodista de datos. *El profesional de la información*, vol. 25, nº2, pp. 286-294.

Lotan, G., Graeff, E., Ananny, M., Gaffney, D., Pearce, I. y Boyd, D. (2011). The Arab Spring | The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions. *International Journal of Communication*, 5, pp. 1375-1405.

LoU Strike Out with International Coalition of Hackers: A Joint Statement by 2600, The Chaos Computer Club, The Cult of the Deadcow, !Hispahack, L0pht Heavy Industries, Phrack and Pulhas (1999, 7 de enero). Disponible en: <http://dasalte.ccc.de/press/releases/1999/CCC19990107.html>, <http://www.cultdeadcow.com/news/statement19990107.html> y <http://www.hispahack.com/oldweb/declara.htm> [Consulta: 26 de marzo de 2014].

Lovink, G. y Riemens, P. (2010). Doce tesis sobre Wikileaks. *CIC Cuadernos de Información y Comunicación*, vol. 16, pp. 139-147.

Lynch, L. (2014). "Oh, WikiLeaks, I would so love to RT you": WikiLeaks, Twitter, and Information Activism. *International Journal of Communication*, 8, pp. 2679–2692.

MacAskill, E. (2010, 19 de diciembre). Julian Assange like a hi-tech terrorist, says Joe Biden. *The Guardian*. Disponible en: <http://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden> [Consulta: 17 de diciembre de 2011].

Magallón Rosa, R. (2012). Wikileaks. ¿Un cambio de paradigma? *Estudios sobre el mensaje periodístico*, vol. 18, nº 1, pp. 127-132.

Mangone, C., Warley, J. (1992). *El Manifiesto. Un género entre el arte y la política*. Buenos Aires: Biblos.

Manion, M. y Goodrum, A. (2000). Terrorism or Civil Disobedience: Toward a Hacktivist Ethic. *Computers and Society* (ACM SIGCAS) 30(2), pp. 14-19.

Manne, R. (2011, marzo). The Cypherpunk Revolutionary: Julian Assange. *The Monthly*. Disponible en: <https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary> [Consulta: 30 de noviembre de 2011].

Marks, P. (2007, 10 de enero). How to leak a secret and not get caught. *New Scientist*. Disponible en: <https://www.newscientist.com/article/mg19325865-500-how-to-leak-a-secret-and-not-get-caught/> [Consulta: 15 de febrero de 2014].

Martínez, J. (2007, 11 de enero). Lanzarán sitio para filtrar documentos gubernamentales. *Sociedad en Red*. Disponible en: <https://wikileaks.org/wiki/Media/Lanzarán_sitio_para_filtrar_documentos_gubernamentales> [Consulta: 22 de febrero de 2014].

Martínez Miguélez, M. (2006). La investigación culitativa (síntesis conceptual). *Revista de Investigación de Psicología*, vol. 9, nº. 1, pp. 123-146.

Masters of Deception (s.f.). *The History of MOD,* vol. I, II, III, IV, V. Disponible en: <http://textfiles.com/hacking/> [Consulta: 31 de julio de 2015].

Maurer, T. (2011). *WikiLeaks 2010: A Glimpse of the Future?* Discussion Paper 2010-2011. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

May, T. (1994, 10 de septiembre). *The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666*. Disponible en: <http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html> [Consulta: 8 de octubre de 2013].

Mayer, R. y Rauber, A. (2011). On wires and cables: Content analysis of WikiLeaks using self-organising maps. En Laaksonen, J. y Honkela T. (eds.), *Proceedings of the 8th Workshop on Self-Organizing Maps (WSOM'11)*, Lecture Notes in Computer Science, vol. 6731, pp. 238-246.

McAthy, R. (2011, 28 de noviembre). Assange accuses editors of being 'corrupted' by power. *Journalism.co.uk*. Disponible en: <http://www.journalism.co.uk/news/assange-accuses-editors-of-being-corrupted-by-power/s2/a546922/> [Consulta: 28 de noviembre de 2011].

McCall, G.J. y Simmons, J.L. (1969). *Issues in Participant Observation: a Text Reader*. Reading, Massachussetts: Addison-Wesley.

McGeveran, W. (2007, 15 de enero). Courts, Injunctions, and WikiLeaks. *Harvard's Info/Law Blog*. Disponible en: <http://blogs.law.harvard.edu/infolaw/2007/01/15/courts-injunctions-and-wikileaks/> [Consulta: 16 de abril de 2014].

McGlynn, K. (2010, 19 de diciembre). 'SNL': Julian Assange Responds To Mark Zuckerberg Being Named 'Person Of The Year' (video). *The Huffington Post*. Disponible en: <http://www.huffingtonpost.com/2010/12/19/snl-julian-assange-zuckerberg_n_798836.html> [Consulta: 9 de diciembre de 2011].

McLuhan, M. (1964). *Comprender los medios de comunicación. Las extensiones del ser humano*. Barcelona: Paidós, 1996.

McLuhan, M. y Nevitt, B. (1972). *Take Today: The Executive As Dropout*. Toronto: Longman.

McNamara, P. (2007, 12 de enero). Here's why Wikileaks is a horrible idea. *Network World*. Disponible en: <http://www.networkworld.com/article/2354110/data-center/here-s-why-wikileaks-is-a-horrible-idea.html> [Consulta, 17 de abril de 2014].

Mendez, T. (2007). WikiLeaks website offers home for whistleblowers, no questions asked. *The West Australian*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

McQuail, D., Blumler, J., Brown, R. (1972). *The television audience: a revised perspective*. En McQuail: *Sociology of Mass Communication*. Harmondsworth: Penguin Books.

Meyer, G. y Thomas, J. (1990). The Baudy World of the Byte Bandit: A Postmodernist Interpretation of the Computer Underground. En F. Schmalleger (ed.) (1990), *Computers in Criminal Justice* (pp. 31-67). Bristol, Indiana: Wyndham Hall Press. Disponible en: <https://w2.eff.org/Net_culture/Postmodernism/byte_bandit.paper>. [Consulta: 15 de junio de 2014].

Meyer, G. y Thomas, J. (eds.). (1992, 11 de noviembre). Cu Digest, #4.57. *Computer Underground Digest*, vol. 4(57). Disponible en: <https://epic.org/security/2600/cu_digest_4.57_2600_raid.html>. [Consulta: 14 de junio de 2014].

Michaels, L. (productor). (2010, 18 de diciembre). *Saturday Night Live: A Message from Mark Zuckerberg and Julian Assange* [programa de televisión]. New York: NBC. Disponible en: <https://www.nbc.com/saturday-night-live/video/a-message-from-mark-zuckerberg/n12987> [Consulta: 10 de diciembre de 2011].

Milan, S. (2013). *Social Movements and their Technologies: Wiring Social Change*. New York: Palgrave MacMillan.

Miller, E. (2012, 11 de julio). Congressional committee holds hearing on national security leak prevention and punishment. *Reporters Committee for Freedom of the Press*. Disponible en: <http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent> [Consulta: 18 de octubre de 2013].

Miller, G. (2010, 22 de diciembre). CIA to examine impact of files recently released by WikiLeaks. *The Washington Post*. Disponible en: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122105498.html> [Consulta: 13 de septiembre de 2013].

Mitnick, K.D. y Simon, W.L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley Publishing.

Mitnick, K.D. y Simon, W.L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. Indianapolis: Wiley Publishing.

Mitnick, K.D. y Simon, W.L. (2011). *Ghost In The Wires: My Adventures as the World's Most Wanted Hacker*. New York: Little, Brown and Company.

Mitra, A. y Schartz, R.L. (2001). From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces. *Journal of Computer Mediated Communication*, 7 (1).

m0j0 (2007, 23 de enero): *Will Wikileaks Keep Anyone Honest?* Musings of an anonymous geek. Disponible en: <http://m0j0.wordpress.com/2007/01/23/will-wikileaks-keep-anyone-honest/> [Consulta: 18 de abril de 2014].

Moglen, E. (1999, 2 de agosto). Anarchism Triumphant: Free Software and the Death of Copyright. *First Monday*, vol. 4, nº 8. Disponible en: <http://firstmonday.org/ojs/index.php/fm/article/view/684/594> [Consulta: 12 de enero de 2014].

Moglen, E. (2003a, enero). *The dotCommunist Manifesto*. Disponible en: <http://moglen.law.columbia.edu/publications/dcm.html> [Consulta: 12 de enero de 2014].

Moglen, E. (2003b, 29 de junio). Freeing the Mind: Free Software and the Death of Proprietary Culture. Disponible en: <http://moglen.law.columbia.edu/publications/maine-speech.html> [Consulta: 13 de enero de 2014].

Mokate, K. (2003). *Convirtiendo el 'monstruo' en aliado: la evaluación como herramienta de la gerencia social*. Serie Documentos de Trabajo I-23. Instituto Interamericano para el Desarrollo Social - INDES. BID. Noviembre. Washington D.C.

Molist, M. (2000, 3 de febrero). La industria del DVD se da de bruces con Internet. Disponible en: <http://ww2.grn.es/merce/2000/decss.html>. [Consulta: 8 de septiembre de 2014].

Molist, M. (2014). *Hackstory.es. La historia nunca contada del underground hacker en la Península Ibérica*. Disponible en: <http://hackstory.es/> [Consulta: 9 de septiembre de 2014].

Mommers, J. (2010). Online Storytelling: Studying Homo narrans in several online habitats by analyzing the framing of the Wikileaks Iraq video in newspapers, blogs and tweets. Paper for the research seminar *Citizen/Journalism: User Generated Content and the Consequences for Journalism*. Module: LJX031M10. Master of Journalism, University of Groningen.

Montagut, A. (1988, 15 de noviembre). Robert Tappan Morris. *El País*. Disponible en: <http://elpais.com/diario/1988/11/15/ultima/595551610_850215.html> [Consulta: 1 de julio de 2014].

Montañés Serrano, M. (2007). Más allá del debate cuantitativo/cualitativo: la necesidad de aplicar metodologías participativas conversacionales. *Revista Política y Sociedad*, vol. 44, nº 1, pp. 13-29.

Moody, G. (2001). *Rebel Code: Linux and the open source revolution*. London: Penguin.

Morales Steger, B., Irisarri Núñez, J.A. y Martín Cavanna, J. (2011). *Esporas de helechos y elefantes. La responsabilidad corporativa de los medios de comunicación por la elaboración de contenidos II. Los diarios nacionales de información general*. Madrid: Fundación Compromiso Empresarial.

Mosco, V. (2004). *The digital sublime: Myth, power and cyberspace*. Cambridge, MA: The MIT Press.

Moses, A. (2007, 20 de enero). Website offers whistleblowers chance to go global. *The Sydney Morning Herald*. Disponible en: <http://www.smh.com.au/news/web/website-offers-whistleblowers-chance-to-go-global/2007/01/19/1169096013302.html> [Consulta: 17 de abril de 2014].

Muller, L. (2010, 9 de diciembre). Visualizing WikiLeaks mirrors. *Multigesture.net*. Disponible en: <http://www.multigesture.net/2010/12/09/visualizing-wikileaks-mirrors/#demo> [Consulta: 2 de diciembre de 2012].

Muñoz-Rojas, O. (2011, 24 de enero). La 'vendetta' de Assange. *El País*. Disponible en: <http://www.elpais.com/articulo/opinion/vendetta/Assange/elpepiopi/20110124elpepiopi_11/Tes> [Consulta: 7 de diciembre de 2011].

Murphy, B.M. (2000a). The founding of APC: Coincidences and logical steps in global civil society networking. *APC Annual Report*, pp. 28-30.

Murphy, B.M. (2000b). Mike Jensen and the code that stitched together the APC: The pre-internet days and early efforts at linking APC nodes. *APC Annual Report*, pp. 31-34.

Murphy, B.M. (2001). *Mapping the pre-history of cyberspace and the making of social movement computer networks, 1973 - 1993* (tesis doctoral). University of Massachusetts Amherst.

Newman, Ch. (1985): *The Post-Modern Aura: The Act of Fiction in an Age of Inflation*. Evanston: Northwestern University Press.

Nissen, J. (1998). Hackers: Masters of Modernity and Modern Technology. En Stefton-Green J. (ed.), *Digital Diversions: Youth Culture in the Age of Multimedia* (pp. 149–71). London: University College London.

Noelle-Neumann, E. (1974). The Spiral of Silence: A Theory of Public Opinion. *Journal of Communication*, vol. 24, issue 2, pp 43-51.

Norris, P. (2001). Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide. New York: Cambridge University Press.

Norton, Q. (2007, 5 de enero). User generated smoking guns. *Wired*. Disponible en: <http://www.wired.com/2007/01/user_generated_/> [Consulta: 17 de abril de 2014].

Norton, Q. (2007, 12 de enero). Wikileaks spilled. *Wired*. Disponible en: <http://www.wired.com/2007/01/wikileaks_spill/> [Consulta: 17 de abril de 2014].

Notes from Nowhere (eds.) (2003). *We Are Everywhere: The Irresistible Rise of Global Anticapitalism*. London, New York: Verso.

Núñez, A. (2007). *¡Será mejor que lo cuentes! Los relatos como herramientas de comunicación.* Barcelona: Empresa Activa.

Nzioka, R. (2007, 24 de enero). Anonymous is the new digital identity. *Flamme d'Afrique*. Disponible en: <https://wikileaks.org/wiki/Media/Anonymous_is_the_New_Digital_Identity> [Consulta: 16 de abril de 2014].

Novo site ajuda anónimos a fazerem denuncias (2007, 18 de enero). *Ciberia*. Disponible en: <https://wikileaks.org/wiki/Media/Novo_site_ajuda_anónimos_a_fazerem_denúncias> [Consulta: 15 de abril de 2014].

O'Harrow Jr., R. (1992, 12 de noviembre). Hackers Allege Harassment at Mall. *The Washington Post*. Disponible en: <https://www.washingtonpost.com/archive/politics/1992/11/12/hackers-allege-harassment-at-mall/5f5e756f-806e-485e-962b-0a5f71635c81/> [Consulta: 30 de julio de 2015).

Oppermann, M. (2000). Triangulation - A Methodological discussion. *International Journal of Tourism Research*, vol. 2, nº 2, pp. 141-146.

Osi (2007, 4 de enero). Düsseldorf Blog con el título Wikileaks - die gefährliche Abschaffung der Geheimnisse. *Düsseldorf Blog*. Disponible en: <http://www.duesseldorf-blog.de/2007/01/04/wikileaks-die-gefaehrliche-abschaffung-der-geheimnisse/> [Consulta: 17 de abril de 2014].

Pacheco, L. (2011). Wikileaks e Internet: O que poderá mudar no jornalismo a partir daqui. *Estudos em Comunicação*, 9, pp. 31-43. LabCom, Laboratório de Comunicação e Conteúdos On-Line. Universidade da Beira Interior, Covilhã, Portugal.

Palin, S. (2010, 29 de noviembre). Serious Questions about the Obama Administration's Incompetence in the Wikileaks Fiasco [comunicación en Facebook]. Disponible en: <https://www.facebook.com/note.php?note_id=465212788434> [Consulta: 16 de diciembre de 2011].

Paquin, B. (1998, 26 de octubre). E-Guerrillas in the mist. *Ottawa Citizen*. Disponible en <http://archive.hrea.org/lists/huridocs-tech/markup/msg00014.html> y <http://www.ainfos.ca/98/oct/ainfos00190.html> [Consulta: 26 de septiembre de 2013].

Partyka, L. (2007, 16 de enero). Serwis Wikileaks: przeciek ujawnisz dyskretnie. *Gazeta.pl*. Disponible en: <https://wikileaks.org/wiki/Media/Serwis_Wikileaks:_przeciek_ujawnisz_dyskretnie> [Consulta: 16 de abril de 2014].

Pegg, S. y E. Berg (2014). Lost and Found: The Wikileaks of De Facto State-Great Power Relations. *International Studies Perspectives*, doi: 10.1111/insp.12078

Peirano, M. (2007, 30 de enero). Wikileaks.org: la 'garganta profunda' de la Red. *Eroski Consumer*. Disponible en: <http://www.consumer.es/web/es/tecnologia/internet/2007/01/30/159251.php> [Consulta: 18 de abril de 2014).

Person, L. (1998). Notes Towards a Postcyberpunk Manifesto. *Nova Express*, 16. Disponible en: <http://slashdot.org/story/99/10/08/2123255/notes-toward-a-postcyberpunk-manifesto> [Consulta: 2 de diciembre de 2011].

Peter, K. (1980). Essay on Hacking. En *The Hacker Papers*, Psychology Today. Disponible en: <http://www.textfiles.com/news/hackpape.hac> [Consulta: 19 de diciembre de 2013].

Pillay, N. (2014, 30 de junio). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, (A/HRC/27/37). Disponible en: <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> [Consulta: 17 de octubre de 2014].

Plaza, M. (2011). *WikiLeaks. La era de los soplones*. Madrid: Atanor Ediciones. Colección Documentos.

Poggiali, T. (2007, 9 de enero). WikiLeaks, il cane da guardia dei governi? *Mytech.it*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Poole, H. (2007, 3 de enero). Wikileaks – interesting to watch in 2007. *CivicActions*. Disponible en: <https://civicactions.com/blog/wikileaks_interesting_to_watch_in_2007> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). Complaining online becomes new social behaviour. *The Star Phoenix*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). Bitch, bitch, bitch online: Got a complaint? There's a site for you as e-tattling grows, whether fair or not. *Windsor Star*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). *Complaining online popular*. *The Leader-Post*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). Are we a bunch of whiners? *Kamloops Daily News*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). Tattlers using the Internet as a weapon: Websites expose all: from leering men to sub-par service. *The Calgary Herald*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). Online whining giving tattlers big audience. *The Halifax Daily News*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> [Consulta: 15 de abril de 2014].

Proudfoot, S. (2007, 22 de enero). E-tattling becomes a new social trend. *Nanaimo Daily News*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_il_cane_da_guardia_dei_governi> y <http://www.canada.com/story.html?id=084eb3a3-1e2b-457c-bee8-7155b5bae93b> [Consulta: 15 de abril de 2014].

Quian, A. (2012, 31 de enero). 'The Huffington Post', periodismo líquido para lasociedad neoliberal. *Sociología crítica. Articulos y textos para debate y análisis de la realidad social*. Disponible en: <http://wp.me/pF2pW-10w> [Consulta: 13 de enero de 2014]. Fuente original: <http://www.mcshuibhne.com/es/2012/01/20/the-huffington-post-periodismo-liquido-para-la-sociedad-neoliberal/>.

Quian, A. (2013a). *El impacto mediático y político de WikiLeaks: la historia más apasionante del periodismo moderno*. Barcelona: Editorial UOC.

Quian, A. (2013b). Supermercados de la información en la era de la transrealidad. *Versión Estudios de Comunicación y Política - Nueva Época*, nº 31, pp. 51-65. Universidad Autónoma Metropolitana Unidad Xochimilco, México.

Quian, A. (2013c, 18 de diciembre). "O nivel de vixilancia en Internet supera o que había na Unión Soviética". Comunicación personal con Richard Stallman publicada en *Galicia Confidencial*. Disponible en: <http://www.galiciaconfidencial.com/noticia/16948-nivel-vixilancia-internet-supera-habia-union-sovietica> [Consulta: 18 de diciembre de 2013].

Ragan, S. (2007, 23 de enero). Summit held for internet code of conduct. *Monsters & Critics*. Disponible en: <http://archive.is/nytM9> y <https://wikileaks.org/wiki/Media/Summit_held_for_internet_code_of_conduct> [Consulta: 16 de abril de 2014].

Ramonet, I. (2011). *La explosión del Periodismo*. Madrid: Clave Intelectual.

Raymond, E.S. (1999). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, California: O'Reilly.

Raymond, E.S. (2001): *How to Become a Hacker*. Thysrus Enterprises. Disponible en: <http://www.catb.org/esr/faqs/hacker-howto.html>. [Consulta: 21 de enero de 2013].

Rey-Mazón, P. *et al*. (2013). PageOneX (Version 1.0) [sofware]. Disponible en: <http://pageonex.com/>.

Rieff, D. (2011). El fin de los secretos: Wikileaks y las guerras digitales por venir. *Letras Libres*, nº 146. Disponible en: <http://www.letraslibres.com/revista/convivio/wikileaks-y-las-guerras-digitales-por-venir>. [Consulta: 9 de diciembre de 2011].

Rockstar dell'anno 2010: Julian Assange. (2010, 13 de diciembre). *Rolling Stone Italia*. Disponible en: <http://www.rollingstonemagazine.it/cultura/notizie/rockstar-dellanno-2010-julian-assange/32161> [Consulta: 2 de diciembre de 2011].

Rosenbaum, R. (1971, octubre). Secrets of the Little Blue Box. *Esquire*. Disponible en: <http://www.historyofphonephreaking.org/docs/rosenbaum1971.pdf> [Consulta: 20 de junio de 2015].

Ruffin, O. (2004, 3 de junio). Hacktivism, From Here to There. *CyberCrime and Digital Law Enforcement Conference*, Yale Law School. Disponible en: <http://www.cultdeadcow.com/cDc_files/cDc-0384.php> [Consulta: 25 de marzo de 2014].

RT. (2011, 16 de marzo): *The man who leaked the world* [archivo de vídeo]. Disponible en: < https://www.rt.com/shows/documentary/assange-leaked-world-dream/> [Consulta: 2 de diciembre de 2011].

Saad Corrêa, E. (2011). Apontamentos sobre o jornalismo extra-muros do Wikileaks. *Contemporanea. Revista de Comunicação e Cultura*, vol. 9, nº 2, pp. 211-230.

Sádaba Rodríguez, I. y Roig Domínguez, G. (2004). Internet: nuevos escenarios, nuevos sujetos, nuevos conflictos. *Nodo50*. Disponible en: <http://www.uned.es/ntedu/asignatu/5-Nodo50.htm> [Consulta: 10 de junio de 2014].

Saiz, E. (2013, 22 de agosto). El soldado Manning, condenado a 35 años de cárcel por las filtraciones a WikiLeaks. *El País*. Disponible en: <http://internacional.elpais.com/internacional/2013/08/21/actualidad/1377090640_718161.html> [Consulta: 14 de diciembre de 2013].

Salmon, C. (2008). *Storytelling. La máquina de fabricar historias y formatear las mentes*. Barcelona: Península.

Salmon, C. (2011). *La estrategia de Sherezade. Apostillas a Storytelling*. Barcelona: Ediciones Península.

Samuel, A. W. (2004). *Hacktivism and the Future of Political Participation* (tesis doctoral). Cambridge, Massachusetts: Harvard University.

Sánchez Hernández, C. (2011). Analogías de la Historia I: Julian Assange y Wikileaks vs Daniel Ellsberg y los pentagon papers. *Nómadas. Revista Crítica de Ciencias Sociales y Jurídica*s, vol. 31, nº 3. Universidad Complutense de Madrid.

Sandberg, J. (1994, 5 de diciembre). Hackers Take Revenge on the Author of New Book on Cyberspace Wars. *The Wall Street Journal*, p. B5.

Sandels, A. (2007, 22 de enero). Whistleblowers now offered an outlet in private - the Wiki way. *The Daily Star Egypt*. Disponible en: <http://www.dailynewsegypt.com/2007/01/22/whistleblowers-now-offered-an-outlet-in-private-the-wiki-way/> [Consulta: 17 de abril de 2014].

Savage, M., y Burrows, R. (2007). The coming crisis in empirical sociology. *Sociology*, 41(5), 885-899.

Schwartau, Winn (2000). *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York: Thunder's Mouth Press.

Sennett, R. (2000). *La corrosión del carácter. Las consecuencias personales del trabajo en el nuevo capitalismo*. Barcelona: Anagrama.

Shimomura, T. y Markoff, J. (1996). *Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw*. New York: Hyperion.

Sieber. S. (1973). The integration of field work and survey methods. *American Journal of Sociology*, 28: 1335-1359.

Scheer, P. (2011, 16 de mayo). Can Mainstream Media Match WikiLeaks? Not Likely. *The Huffington Post*. Disponible en: <http://huff.to/ihZqr4> [Consulta: 7 de diciembre de 2011].

Schmidt, T.S. (2007, 22 de enero). A Wiki for Whistle-Blowers. *Time*. Disponible en: <http://content.time.com/time/nation/article/0,8599,1581189,00.html> [Consulta: 16 de abril de 2014].

Sengupta, S. (2011, 10 de noviembre). *Twitter Ordered to Yield Data in WikiLeaks Case*. *The New York Times*. Disponible en: <http://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html> [Consulta: 16 de febrero de 2014].

Shah, N. (2011, 24 de abril). Who the Hack? *Indian Express*. Disponible en: <http://www.indianexpress.com/news/who-the-hack/779496/> [Consulta: 8 de diciembre de 2011].

Siddique H. y Weaver, M. (2010, 1 de diciembre). US embassy cables culprit should be executed, says Mike Huckabee. *The Guardian*. Disponible en: <http://www.theguardian.com/world/2010/dec/01/us-embassy-cables-executed-mike-huckabee> [Consulta: 18 de diciembre de 2011].

Slatalla, M. y Quittner, J. (1995). *Masters of Deception: The Gang that Ruled Cyberspace*. New York: Harper Collins.

Small Poppy TV (2010, 20 de diciembre). *Oprah in Australia - Julian Assange interview* [archivo de vídeo]. Disponible en: <http://youtu.be/TtsoxxCsY0I> [Consulta: 30 de noviembre de 2011].

Smith, H.W. (1975*). Strategies of Social Research: The methodological imagination*. London: Prentice Hall.

Smith, J.K. (1983). Quantitative versus Qualitative Research: An Attempt to Clarify the Issue. *Educational Researcher*, vol. 12, nº 3, pp. 6-13.

Snickars, P. (2014). Himalaya of Data. *International Journal of Communication*, 8, pp. 2666–2678.

"Sobramos la mitad de los periodistas", afirma Bieito Rubido, director de 'ABC'. (2011, 24 de noviembre). *El Mundo*. Disponible en: <http://www.elmundo.es/elmundo/2011/11/24/comunicacion/1322138353.html > [Consulta: 5 de noviembre de 2013].

Söderberg, J. (2009). Hackers GNUnited! En Stian Eide (ed.), *Free Beer* (pp. 89-105). Göteborg: Lulu.

Solís, J. (2011, 3 de mayo). Julian Assange: A Modern Day Hero? Inside the World of WikiLeaks. *PopMatters*. Disponible en: <http://www.popmatters.com/pm/review/140193-julian-assange-a-modern-day-hero-inside-the-world-of-wikileaks/> [Consulta: 8 de diciembre de 2011].

Springer, S, Chi, H, Crampton, J, McConell, F, Cupples, J, Glynn, K,… Attewell, W. (2012). Leaky geopolitics: The ruptures and transgressions of WikiLeaks. *Geopolitics*, 17(3), 681-711.

Star, A. (ed.) (2011). *Open Secrets: WikiLeaks, War, and American Diplomacy*. New York: The New York Times.

Suárez Puerta, B.L. (2009). Reflexiones sobre la enseñanza en situaciones transmediales. *Revista Investigación y Reflexión*, vol. XVII, nº 2, diciembre, pp. 183-198. Facultad de Ciencias Económicas, Universidad Militar Nueva Granada, Colombia.

Stabe, M. (2007, 4 de enero). A wiki for leaking secrets. *Martinstabe.com*. Disponible en: <http://www.martinstabe.com/2007/01/04/a-wiki-for-leaking-secrets/ > [Consulta: 8 de diciembre de 2011].

Stalbaum, B. (1998). *The Zapatista Tactical FloodNet*. Electronic Civil Disobedience. Disponible en: <http://www.thing.net/~rdom/ecd/ZapTact.html> [Consulta: 30 de septiembre de 2014].

Stallman, R. (1985). The GNU Manifesto. *Dr. Dobb's Journal of Software Tools*, vol. 10, nº 3. Disponible en: <http://www.gnu.org/gnu/manifesto.en.html>. [Consulta: 18 de enero de 2014].

Stallman, R. (2000). On Hacking. Disponible en: <https://stallman.org/articles/on-hacking.html>. [Consulta: 19 de enero de 2014].

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books. Disponible en: <https://ebooks.adelaide.edu.au/s/sterling/bruce/hacker/> y <http://www.mit.edu/hacker/hacker.html> [Consulta: 10 de septiembre de 2013].

Sternstein, A. (2007, 4 de enero). Forthcoming 'Wiki' Aims To Leak, Analyze Documents. *National Journal's Technology Daily*. Disponible en: <http://cryptome.org/wikileaks/wikileaks-leak.htm> y <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 14 de abril de 2014].

Symington, A. (2009, 1 de septiembre). Exposed: Wikileaks' secrets. *Wired*. Disponible en: <http://www.wired.co.uk/magazine/archive/2009/10/start/exposed-wikileaks-secrets> [Consulta: 14 de junio de 2014].

Takhteyeva, Y., Gruzdb, A. y Wellmanc, B. (2012). Geography of Twitter Networks. *Social Networks*, 34, pp. 73-81

Taylor, P. (1999). *Hackers: crime in the digital sublime*. London: Routledge.

Taylor, P. (2004). Hacktivism: Resistance is fertile? En C. Summer (ed), *The Blackwell companion to criminology* (pp. 486-500). Massachusetts: Blackwell Publishing.

The Abuse of Private Manning (2011, 14 de marzo). *The New York Times*. Disponible en: <http://www.nytimes.com/2011/03/15/opinion/15tue3.html> [Consulta: 13 de diciembre de 2013].

The Mentor (1986, 8 de enero). The Conscience of a Hacker. *Phrack*, vol. 1, issue 7, phile 3 of 10. Disponible en: <http://phrack.org/issues/7/3.html#article> [Consulta: 10 de julio de 2013].

The on-line hacker Jargon File, version 4.4.7. (2003, 29 de diciembre). Raymond, E.S. (ed). Disponible en: <http://www.catb.org/jargon/html/>. [Consulta: 20 de enero de 2012].

The Pew Research Center for the People & the Press (2011). *Views of the News Media: 1985-2011*. Washington: Pew Research Center.

Thelwall, M., Wouters, P. y Fry, J. (2008). Information-centred research for large-scale analysis of new information sources. *Journal of the American Society for Information Science and Technology*, 59(9), 1523-1527.

Thessdept (2010, 16 de diciembre): *Julian Assange: The Outsider - The WikiLeaks movie tráiler* [archivo de vídeo]. Disponible en: <http://youtu.be/Qc08KyYYRgI>. [Consulta: 30 de noviembre de 2011].

Thomas, D. (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.

Thierer, A. y Szoka, B. (2009, 12 de agosto). Cyber-Libertarianism: The Case for Real Internet Freedom. *The Technology Liberation Front*. Disponible en: <http://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet-freedom/> [Consulta: 4 de octubre de 2013].

Toffler, A. (1980). *The Third Wave*. New York: Bantam Books.

Tool, Theodore T. (1991, 1 de septiembre). *MIT Guide to Lock Picking*. Disponible en: <http://www.lysator.liu.se/(bw)/mit-guide/MITLockGuide.pdf> [Consulta: 30 de junio de 2014].

Toret, J. (coord.) (2013). *Tecnopolítica: la potencia de las multitudes conectadas. El sistema red 15M, un nuevo paradigma de la política distribuida*. Barcelona: UOC-IN3.

Torvalds, L. y Diamond, D. (2001). *Just For Fun: The Story of an Accidental Revolutionary*. New York: HarperCollins Publisher.

Touraine, A. (1969). *La Societé post-industrielle*. París: Denöel.

Trecet, R. (2011, 18 de octubre). "Un periodista vale hoy su número de followers". *Jot Down*. Disponible en: <http://www.jotdown.es/2011/10/ramon-trecet-un-periodista-vale-hoy-su-numero-de-followers/> [Consulta: 17 de octubre de 2012].

Trueman, M. (2011, 9 de noviembre*).* Julian Assange, the opera: Wikileaks brought to book. *The Guardian*. Disponible en: <http://www.theguardian.com/stage/2011/nov/09/julian-assange-the-opera> [Consulta: 20 de diciembre de 2011].

Turkle, S. (1984). *The Second Self: computers and the human spirit*. 20th anniversary edition, 2005. Cambridge: The MIT Press.

Turkle, S. (2012). *Alone together: Why we expect more from technology and less from each other*. New York: Basic books.

Twitter (2010). *Twitter 2010: Year in review*. Disponible en: <http://yearinreview.twitter.com/2010/> [Consulta: 1 de diciembre de 2011].

Un site internet pune în pericol documentele guvernamentale din întreaga lume (2007, 24 de enero). *Adevarul*. Disponible en: <http://adevarul.ro/news/societate/un-site-internet-pune-pericol-documentele-guvernamentale-intreaga-lume-1_50ac1c447c42d5a66384ec60/index.html> [Consulta: 17 de abril de 2014].

Ugander, J., Backstrom, L., Marlow, C. y Kleinberg, J. (2012). Structural diversity in social contagion. *Proceedings of the National Academy of Sciences*, USA, 109(16), pp. 5962-5966.

United Press International. (2007, 15 de enero). Wikileaks to serve as online Deep Throat. Disponible en: <http://www.upi.com/Odd_News/2007/01/15/Wikileaks-to-serve-as-online-Deep-Throat/UPI-67551168897384/> [Consulta: 16 de abril de 2014].

Uricchio, W. (2014). True Confessions: WikiLeaks, Contested Truths, and Narrative Containment. *International Journal of Communication*, 8, pp. 2567–2573.

Uysal, N. (2011). The Battle of WikiLeaks: Mass Self-Communication, Hacker Culture, and Financial Institutions. *Proceedings of the 24th annual International Association for Conflict Management (IACM)*, Istanbul, Turkey.

Varela, J. (2006, 21 de diciembre). La amenaza de la paradoja del control. *Periodistas21*. Disponible en: <http://periodistas21.blogspot.com/2006/12/la-amenaza-de-la-paradoja-del-control.html> [Consulta: 22 de noviembre de 2012].

Varela, J. (2011, 12 de diciembre). El País franquicia el Huffington Post. *Estrella Digital*. Disponible en: <http://www.estrelladigital.es/blogs/juan_varela/Pais-franquicia-Huffington-Post_7_1083561638.html> [Consulta: 22 de noviembre de 2012].

Vegh, S. (2003). *Hacking for Democracy: A Study of the Internet as a Political Force and Its Representation in the Mainstream Media* (tesis doctoral). University of Maryland, College Park.

Velkova, (2011). WikiLeaks CableGate and the Multi-Stakeholder Model of Internet Governance. *Communication for Development (ComDev 09)*, Malmö University.

Vespignani, A. (2009). Predicting the behavior of techno-social systems. *Science*, 325, 425-428.

Vicent, M. (2010, 12 de diciembre). Prometeo. *El País*. Disponible en: <http://elpais.com/diario/2010/12/12/ultima/1292108401_850215.html> [Consulta: 26 de noviembre de 2011].

Vidal Vega, J. y Romero Portillo, J. (2010). La denuncia social en Internet: Wikileaks y la filtración de documentos secretos. *Actas II Congreso Internacional Latina de Comunicación Social*, Universidad La Laguna.

Villeda Saldaña, D. (2011). Julian Assange: Periodismo científico, conspiración y ética hacker. *Quehacer*, nº 181, Lima, enero-marzo, pp. 58-69.

Vinter, H. (2011, 21 de septiembre). Charlie Beckett: WikiLeaks symptomatic of a trend that's going to accelerate. *Editors Weblog*. Disponible en: <http://www.editorsweblog.org/2011/09/21/charlie-beckett-wikileaks-symptomatic-of-a-trend-thats-going-to-accelerate> [Consulta: 1 de diciembre de 2011].

Voss, B. (2007, 20 de enero). Ich verrate Ihnen jetzt mal was!; Wikis jüngster Ableger sammelt angebliche Geheimdokumente. *Süddeutsche Zeitung*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta:15 de abril de 2014].

Waites, R. (2011, 20 de octubre). La máscara de 'V de Vendetta': ¿qué hay detrás? *BBC Mundo*. Disponible en: <http://www.bbc.co.uk/mundo/noticias/2011/10/111020_mascara_v_vendetta_az.shtml> [Consulta: 12 de diciembre de 2011].

Wark, M. (2004). *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Weber, M. (1992). *The Protestant Ethic and the Spirit of Capitalism*. London: Routledge.

Weizenbaum, J. (1976). *Computer Power and Human Reason: From Judgment To Calculation*. San Francisco: W. H. Freeman.

Weng, L., Flammini, A., Vespignani, A. y Menczer, F. (2012). Competition Among Memes in a World with Limited Attention. *Nature Scientific Reports*, 2(335).

White, M. (2002). Representations or people? *Ethics and Information Technology*, 4(3), pp. 249-266.

Website wants to take whistleblowing online (2007, 11 de enero). *CBC News*. Disponible en: <http://www.cbc.ca/news/technology/website-wants-to-take-whistleblowing-online-1.692164> [Consulta: 16 de abril de 2014].

Werner, H. (2007, 25 de enero). Geheimnisverrat bei Wikileaks. *Die Welt*. Disponible en: <http://www.welt.de/print-welt/article711145/Geheimnisverrat_bei_Wikileaks.html> [Consulta: 16 de abril de 2014].

Why We Protest (Italian Edition!). (2008, 9 de marzo). Disponible en: <https://whyweprotest.net/threads/why-we-protest-italian-edition.3014/> [Consulta: 16 de febrero de 2014].

Wiki. (2015, 2 de octubre). Wikipedia. Disponible en: <https://es.wikipedia.org/wiki/Wiki> [Consulta: octubre 4 e octubre de 2015].

WikiLeaks. (2011a, 1 de septiembre). Global - Guardian journalist negligently disclosed Cablegate passwords. Disponible en: <https://wikileaks.org/Guardian-journalist-negligently.html> [Consulta: 1 de diciembre de 2011).

WikiLeaks. (2011b, 24 de octubre). Banking Blockade. Disponible en: <https://www.wikileaks.org/Banking-Blockade.html> [Consulta: 10 de mayo de 2014].

WikiLeaks. (2013, 2 de julio). *Edward Snowden submits asylum applications*. Disponible en: <https://wikileaks.org/Edward-Snowden-submits-asylum.html>. [Consulta: 3 de mayo de 2014].

WikiLeaks anuncia la publicación de todos sus cables diplomáticos sin proteger a sus fuentes. (2011, 2 de septiembre). *El País*. Disponible en: <http://internacional.elpais.com/internacional/2011/09/02/actualidad/1314914403_850215.html> [Consulta: 30 de noviembre de 2011].

Wikileaks, a másként gondolkodóknak. (2007, 21 de enero). *Sg.hu*. Disponible en: <https://sg.hu/cikkek/49935/wikileaks_a_maskent_gondolkodoknak> [Consulta, 17 de abril de 2014].

WikiLeaks, documenti segreti. (2007, 16 de enero). *La Stampa*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks_documenti_segreti> [Consulta: 16 de abril de 2014].

WikiLeaks, le partage Internet des dissidents. (2007, 12 de enero). *Marketing Etudiant*. Disponible en: <https://wikileaks.org/wiki/Media/WikiLeaks,_le_partage_Internet_des_dissidents> [Consulta: 16 de abril de 2014].

Wikileaks - the truth is in there… somewhere. (2007, 16 de enero). *bROkeN siMuLAcRA*. Disponible en: <https://wikileaks.org/wiki/Media/Wikileaks_the_truth_is_in_there_somewhere> [Consulta: 17 de abril de 2014].

WikiLeaks Leak. (2007, 7 de enero). *Cryptome*. Disponible en: <http://cryptome.org/wikileaks/wikileaks-leak.htm> [Consulta: 14 de marzo de 2014].

WikiLeaks Leak 2. (2007, 9 de enero). *Cryptome*. Disponible en: <https://cryptome.org/wikileaks/wikileaks-leak2.htm> [Consulta: 14 de marzo de 2014].

Wikileaks.org: kiszivárogtatási portál nemcsak újságíróknak. (2007, 22 de enero). *Transindex*. Disponible en: <http://tech.transindex.ro/?hir=4637> [Consulta: 18 de abril de 2014].

Wikileaks: Collective Intelligence Agency? (2007, 23 de enero). *Valeurdusage.net*. Disponible en: <https://wikileaks.org/wiki/Media/Collective_Intelligence_Agency> [Consulta: 16 de abril de 2014].

Wikipedia inspira denúncia anônima na web. (2007, 15 de enero). en *G1 - Globo*. Disponible en: <https://wikileaks.org/wiki/Media/Wikipedia_inspira_ denúncia _ anônima _na_web> [Consulta: 16 de abril de 2014].

Wikipedia. (2015, 30 de septiembre). Wikipedia. Disponible en: <https://es.wikipedia.org/w/index.php?title=Wikipedia&oldid=89206782> [Consulta: 4 de octubre de 2015].

WikiWikiWeb. (2015, 30 de agosto). Wikipedia. Disponible en: <https://en.wikipedia.org/wiki/WikiWikiWeb> [Consulta: 4 de octubre de 2015].

Wiki Wiki Web (s.f.). Wiki Wiki Web. Disponible en: <http://c2.com/cgi/wiki/wiki?WikiWikiWeb> [Consulta: 4 de octubre de 2013].

Williamson, E. (2007, 15 de enero). Freedom of Information, the Wiki Way. *The Washington Post*. Disponible en: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/14/AR2007011400760.html> [Consulta: 15 de abril de 2014].

Witzel, D. (2007, 15 de enero). Wikileaks: More transparency for the policy common. *Online Community Report*. Disponible en: <https://wikileaks.org/wiki/Media/Wikileaks:More_transparency_for_the_policy_commons> [Consulta: 16 de abril de 2014].

Wivel, P. (2007, 30 de enero). Revolution via nettet: ny central for afsloerende dokumenter. *Politiken*. Disponible en: <https://wikileaks.org/wiki/Media/Unsorted_articles> [Consulta: 15 de abril de 2014].

Wolf, M, (1987). *La investigación en la comunicación de masas: críticas y perspectivas*. Barcelona: Paidós, 1996.

Wolton, D. (2000). *Internet, ¿y después?* Barcelona: Editorial Gedisa.

Wozniak, S. (2014, 29 de septiembre). The man who made Apple possible is in trouble —and you can help him. *Gizmodo*. Disponible en: <http://gizmodo.com/the-man-that-made-apple-possible-is-in-trouble-and-you-1640196741> [Consulta: 11 de diciembre de 2014].

Wray, S. (1998). Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics. Switch, vol. 4, nº 2. Disponible en: < http://switch.sjsu.edu/web/v4n2/stefan/> [Consulta: 21 de septiembre de 2013].

Wray, S. (1999). On Electronic Civil Disobedience. *Peace Review*, vol. 11, nº 1, pp. 107-111.

Wu, S., Hofman, J.M., Mason, W.A., Watts, D.J. (2011). Who Says What to Whom on Twitter. *Hyderabad: 20th Annual World Wide Web Conference*, ACM, India.

Yuste, B. (2011). Del 11-M a Wikileaks, la revolución política en internet. *Cuadernos de Comunicación Evoca, 4 (Comunicación política 2.0)*, pp. 41-45.

Zambardino, V. (2007, 7 de enero). Il wikiventilatore? fa paura. *La Repubblica*. Disponible en: <https://wikileaks.org/wiki/Media/Il_wikiventilatore 7 de enero Vittorio Zambardino> [Consulta: 15 de abril de 2014].

Zetter, K. (2010, 30 de julio). WikiLeaks Posts Mysterious 'Insurance' File. *Wired*. Disponible en: <http://www.wired.com/threatlevel/2010/07/wikileaks-insurance-file/> [Consulta: 12 de diciembre de 2011].

Zimbardo, P.G. (1980). The hacker papers. *Psychology Today*, agosto, pp. 64-69.

Žižek, S. (2007, 26 de enero). In You More Than Yourself. *In this Times*. Disponible en: <http://www.inthesetimes.com/article/3003/in_you_more_than_yourself/> [Consulta: 7 de diciembre de 2011].

Žižek, S. (2011). Good Manners in the Age of WikiLeaks. *London Reviews of Book*, vol. 33, nº 2, 20 de enero, pp. 9-10.

ع هق ر شن فظ راطي هق ي حول ل م عل ل(2007, 11 de enero). *Al-Arab*. Disponible en: <http://www.alarab.com/Article/9101> [Consulta: 18 de abril de 2014].

לעשות עולם טוב יותר (2007, 12 de enero). *Notes.co.il*. Disponible en: <https://wikileaks.org/wiki/Media/לעשות_עולם_טוב_יותר> [Consulta: 16 de abril de 2015].

сделай информацию свободной, организуй утечку данных! (2007, 12 de enero). *openPGP в Россuu*. Disponible en: <https://www.pgpru.com/novosti/2007/0112wikileaksorgsdelajjinformacijusvobodnojjorganizujjutechkudannyh> [Consulta: 18 de abril de 2014].

"圧政を敷く国々"を告発するWikileaks (2007, 24 de enero). *ITmedia*. Disponible en: <https://wikileaks.org/wiki/Media"圧政を敷く国々"を告発するWikileaks> [Consulta: 16 de abril de 2014].

情報漏洩用Wiki「ウィキリークス」近日オープン予定 (2007, 13 de enero). *Slashdot.jp*. Disponible en: < https://wikileaks.org/wiki/Media/情報漏洩用Wiki「ウィキリークス」近日オープン予定> [Consulta: 16 de abril de 2015].

異議份子出資／Wikileaks網站推動良知洩密運動 (2007, 16 de enero). *Liberty Times Net*. Disponible en: <http://news.ltn.com.tw/news/world/paper/111618> [Consulta: 18 de abril de 2014].

LISTA DE CUADROS

LISTA DE GRÁFICOS

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

ANEXOS

ANEXO I: Sitios web espejo de WikiLeaks (actualizado: 15-12-2010)

wikileaks.as50620.net
freeus.jsdev.org
wl.donatepl0x.com
wikileaks.ptitlu.org
wikileaks.morningtime.com
wikileaks.gonte.se
leaks.gooby.org
wikileaks.harvo.de
wikileaks.81-89-98-125.blue.kundencontro...
wikileaks.joworld.net
wikileaks.mantrain.me
wikileaks.adhelis.com
wl.alfeldr.de
wikileaks.geekview.be
wikileaks.dysternis.de
wikileaks.krkr.eu ipv6
wikileaks.theunfamiliar.co.uk
wikileaks.aelmans.eu
wl.ernstchan.net
zwartemarktplaats.com
wikileaks.subastas-xxx.com
wikileaks.fernandoramirez.com.ar
www.wikileaks.freelists.com.au
wleaks.3sge.pulsedmedia.com
wikileaks.razor1911.com
wikileaks.trankil.info
wikileaks.timburke.org
wikileaks.myscripts24.de
wikileaks.ruicruz.pt
wikileaks.nerdpol.org ipv6
www.wikileakz.eu
wikileaks.superjoesoftware.com
mirror1.wikileaks.lu
internaluse.net
brd.mcbf.net
wikileaks.1407.org
azow.selb.us
wikileaks.nortemagnetico.es
skaelikiw.info
vm8157.vps.tagadab.com
wikileaks.noomad.org
wikileaks.infinium.org.uk
wikileaks.sirobert.com
wikileaks.marktaff.com
wikileaks.aamjanata.com
wikileaks.julietvanree.com
wikileaks.tard.is
wikileaks.cellue.de
wikileaks.challet.eu
wikileaks.rolisteam.org
wikileaks.renout.nl
wikileaks.kaptenkong.se
wikileaks.dubronetwork.fr ipv6
wikileaks.sbr.im
www.fuckip.de
www.wlmirror.com
wikileaks.rout0r.org
wikileaks.high-color.de
wikileaks.jikan.fr
wikileaks.fs-cdn.net
wikileaks.nulset.net
wl.yoltie.net
wikileaks.vixns.net
wikileaks.serverius.net
leaks.zero-internet.org.uk
wikileaks.dena-design.de
cablegate.askedo.de
wikileaks.chmod.fi
leaked.rndm.ath.cx
wleaks.hellfire.pulsedmedia.com
wikileaks.dokansoft.com.ar
wikileaks.gonte2.nu
wikileaks.ehcdev.com
wikileaks.breit.ws
wikileaks.now-pages.com
cablegate.r3blog.nl ipv6
wikileaks.realprogrammer.org
wikileaks.rtjuette.de
mirror2.wikileaks.lu
wikileaks.r00t.la
wikileaks.merciful.nl
wl.datendetektei.de ipv6
wikileaks.furdev.org
wikileaks.threefingers.ca
www.anontalk.com
nl1.wikileaksmirror.nl
wikileaks.xcplanet.com
wikileaks.piratskasit.cz
wikileaks.solvare.se
wikileaks.hmaks.com
www.wikigoteo.dialetheia.net
wikileaks.argenton.ch
wikileaks.enzym.su
wl.opsec.eu ipv6
wikileaks.kister.org
wl.gernox.de
wikileaks.fdn.fr
wikileaksmirror.proxelsus-hosting.deipv6
wikileaks.perry.ch
wikileaks.u0d.de
wikileaks.psytek.net
wikileaks.chiquitico.org
www.gruiiik.org
wikileaks.holarse-linuxgaming.de
wikileaks.huissoud.ch
wikileaks.burnzone.de
wikileaks.franslundberg.com
wikileaks.gnourt.org
wikileaks.zeitkunst.org
wikileaks.synssans.nl
wikileaks.yasaw.net
wikileaks.zone84.net
wikileaks.iuwt.fr
wlmirror.wildeboer.net
wikileaks.splichy.cz
wikileaks.palisades-berlin.de
wikileaks.thinkfurther.de
leaks.stumcomie.com
wikileaks.zurk.org
wikileaks.emilts.com
wikileaks.ego-world.org
wikileaks.footboot.net
wikileaks.the-secret-world.info
wikileaks.rustigereigers.nl
wikileaks.emptyflask.net
wikileaks.cordover.id.au
wikileaks.spurious.biz
wikileaks.mollar.me
wikileaks.datkan.net ipv6
wikileaks.brenne.nu ipv6
wikileaks.hutonline.nl
wikileaks.jawawa.net
www.wikileaks.nw-ds.com
peoplerule.info
www.hit-repeat.net
im.wikileak.im
wikileaks.dft-labs.eu
wikileaks.i0i.co

wikileaks.lionelwood.com
wikileaks.diedx.nl
wikil3aks.dyndns.org
wikileaks.mcpond.co.nz
wikileaks.digitalevuilnisman.nl
wikileaks.syncaddict.net
info.patourie-systems.com
wikileaks.brokenbydesign.org
wikileaks.kronoss.org
wikileaks.nperfection.com
wikileaks.laquadrature.net
wikileaks.39mm.net
wikileaks.krtek.net
wikileaks.explain-it.org
wikileaks.dunnewind.net
wikileaks.datenscheibe.org
wikileaks.nodemaster.de
wikileaks.sedrati-dinet.net
wikileaks.tonbnc.fr
wikileaks.spinrise.com
wikileaks.lainconscienciadepablo.net
wikileaksmirror.matstace.me.uk
wikileaks.junkle.org
wikileaks.karlsen.co
wikileaks.azatoth.net
wikileaks.back2hack.cc
wl.treymassingill.com
wikileaks.rickfalkvinge.se
wikileaks.freei.me
wikileaks.iheartfreedom.ca
wikileaks.excds.se
ichbinauchwikileaks.org ipv6
cablegate.dyndns.info
wikileaks.emquadat.com
wikileaks.urli.eu
w.mtga.me
wikileaks.citizen-boycott.org
wl.rekursion.ch
wikileaks.cimeterre.info
wikileaks.crypton-technologies.net
wl.creative-guerillas.com
wikileaks.blogator.de
wikileaks.concretedonkey.cz.cc
wikileaks.webterrorist.net
wikileaks.theano.de
wikileaks.caseid.org
wikileaks.atpolitics.com
wikileaks.tetalab.org
wikileaks.atpolitics.com
www.wikileaks.videoteppista.net
wikileaks.mitov.eu
wikileaks.stephaneerard.fr
wikileaks.thearksakura.com
wikileaks.antifan.de ipv6
wikileaks.chram.net
wikileaks.encgmail.com
wikileaks.siwhine.org
wikileaks.delight.ch
www.hallitus.info
wikileaks.softic.cz
wikileaks.nisd.dk
wikileaks.s4ku.com
wikileaks.invisihosting.com
wikileaks.legrandsoir.info
leaks.uaqv.com
www.emilts.com
88.80.28.74
wl.fcharlier.net
wikileaks.kapitein.org
wikileaks.listepik.net
wikileaks.rigacci.org
cablegate.sentientrobot.net
wikileaks.rothnet.org
wikileaks.g33kthug.co.uk
87.106.58.253
leaks.iamfos.co
wikileaks.lupine.me.uk ipv6
wl.unbloggbar.org
wikileaks.supercrapule.com
wikileaks.poliisi.mobi
wikileaks.amette.eu
wikileaks.chsdl.de
wikileaks.rackstack.com
wikileaks.under.ch
wikileaks.nldla.com
wikileaks.afturgurluk.org
wikileaks3.no-ip.org
wikileaks.laotracarboneria.net
wleaks.shellmix.com
wikileaks.in-edv.de
naixt-genne.com
wikileaks.2qt.us
wikileaks.xgstatic.fr
wikileaks.philpep.org ipv6
wikileaks.outcast.no
wikileaks.oualid.net
wl.22web.net
wikileaks.buzzworkers.com
wikileaks.luchaspopulares.org
wikileaks.otnf.tk
leaks.letsneverdie.net
wlfreedom.info
wikileaks.deutero.org
wikileaks.tamcore.eu
wikileaks.jotocorp.com
wikileaks.org.org
wasiutynski.net
wikileaks.fuzziesoftware.com
wikileaks.yoerin.nl
wikileaks.schroth.cx
wikileaks.moochm.de
wikileaks.thejosh.info
wikileaks.redhog.org
wikileaks.sentientrobot.net
wikileaks.glembotzky.com
wikileaks.mkristian.de
wikileaks.artwww.net
wikileaks.kevn.de
leaks.3nglish.co.uk
wikileaks.cathomen.org
wikileaks.poete.eu.org ipv6
www.wikileaks.djity.net
wikileaks.explain-it.org
wikileaks.ratm.ch
wikileaks.dunwich.org
wikileaks.webtito.be ipv6
wikileaks.b166er.net
wikileaks.virii.lu
wikileaks.wass-media.com
wikileaks.webprofiles.org
santocristo.info
wikileaks.bandaancha.eu
wikileaks.karlsen.co
wikileaks.batsh.it
last.to
wikileaks.serverlicious.org
leaks.kooll.info
wikileaks.ic.cz
wikileaks.phasebook.net
wikileaks.hermans.net
wikileaks.datapusher.net
wikileaks.funkcentral.de
wl.hor.de
wikileaks.aircraftdispatch.net
wikileaks.rhgnet.de
wikileaks.medienfuzzis.com
wikileaks.para-dice.de
wikileaks.bandsal.at ipv6
wikileaks.zarovka.com
wikileaks.deepdata.de
wikileaks.electric-castle.net
wikileaks.paysen.net
wikileaks.nslu2-info.de
wikileaks.yasaw.net
mhym.de
wikileaks.grokia.se
wikileaks.youfailed.de
wikileaks.canariaswireless.net
wikileaks.a-dit.fr

wikileaks.thefrackin.info
wikileaks.simplaza.net
www.helpwikileaks.co.za
wikileaks.sphardy.com
wikileaks.sodom.se
wikileaks.a4r.com.mx
wl-mirror.sokoll.com
wikileaks.giggsey.com
wikileaks.unknowntruth.net
wl.kaizer.se
wikileaks.kyak106.com
wikileaks.leech.it
wikileaks.0x04.com
wl.sairyx.org
wikileaks.chpwn.com
wikileaks.slackdev.com
wikileaks.efremigio.es
wikileaks.freedomofspee.ch
wikileaks.chuso.net
wleaks.fryking.se
wikileaks.0xff.it
wikileaks.revspace.nl
wikileaks.kassala.de
wikileaks.svartasegel.se
wikileaks.waixan.se
wikileaks.hackety.net
leaks.freudian.sl
wikileaksmirror.ch
74.63.248.219
wikileaks.liberal-venezolano.net
wikileaks.orfeu.es
wikileaks.noova.de ipv6
wikileaks.pesqair.com
wikileaks.byteserv.de
wikileaks.popcnt.org
wikileaks.adoutte.com
wikileaks.roethof.net ipv6
wikileaks.apathie.net
www.wikileaks.ufone.de
wikileaks.eglin.net
wikileaks.pwnt.nl
www.wikileaks.queray.com
wikileaks.extensity.co.nz
wikileaks.beobach.de
wikileaks.nc23.de
wikileaks.cloudyks.org
wikileaks.teamdragonball.de
mirror.friendsofwikileaks.org.uk
wikileaks.adundo.com
wikileaks.tollofsen.se
wikileaks.moell.us
www.priv.us
www.finngaria.de
wikileaks.maero.dk
gouv.delation.org
wl.dixon.pl
wikileaks.wkellner.com
wikileaks.nethazard.eu
wikileaks.damn1337.de
wikileaks.224charenton.net
wl.kallix.net ipv6
wikileaks.opperschaap.net
wikileaks.legalsutra.org
wikileaks.lillem4n.se
wikileaks.pamphleteer.de
wikileaks.mirror.jfet.org
wikileaks.3ofcoins.net
wikileaks.fuck.cc
wikileaks.openmafia.org
wikileaks.zanooda.com
www.elajt.info
wikileaks.letras.net
wikileaks.mazurinka.ru
wikileaks.apileofbytes.com
leaks.curaj.tv
wikileaks.mairipa.com
wikileaks.crome.us
wikileaks.k-ribou.com
wikileaks.milchi.de
wikileaks.laez.nl
wikileaks.piratenpartei-nrw.de
wl.ownage4u.nl
cablegate.dig-and-be-dug.com
www.wikileaks.cat
wikileaks.leckerbits.com
wikileaks.nicolbolas.org ipv6
wikileaks.zro.co
wikileaks.acm.jhu.edu
wikileaks.iodev.org
wikileaks.thespinlight.com
team-moh.nl
wikileaks.mooo.se
kileaks.byethost6.com
majjj.com
wikileaks.swissbite.net ipv6
wikileaks.rudemusic.net
dgmx2k.dyndns.org:800
wikileaks.users.feralhosting.com
wikileaks.systemcreators.org
wl.mrblue.name
wikileaks.disknode.org
wikileaks.lazzurs.net
wikileaks.brokenco.de
wikileaks.classcast.de
wikileaks.neopt.org
wikileaks.skvorsmalt.cz ipv6
wikileaks.metrogeek.fr
wikileaks.fellr.net
wikileaks.zombix.pcriot.com
wl.thj.no
wikileaks.macventure.de
wikileaks.bitciple.com
help.majestan.com
wikileaks.scripter.se
wikileaks.discipulosdopinguim.com.br
wikileaks.kitara.nl
wikileaks.marpeck.net
wikileaks.return0.de
wikileaks.nerdhero.org
wikileaks.g0rn.com
wikileaks.hoppipolla.net
wikileaks.paper.st
wikileaks.wtfstfu.org
wl.ito315.com
wikileak.eicat.ca
wl.23tube.org
wikileaks.herrschaftsfrei.org
wikileaks.mumu.cz
wikileaks.zilog.es
wikileaks.chpwn.com
wikileaks.stasi.fi
wl.kollegstufe.org
wikileaks.intresseklubben.org
wikileaks.dexite.de
wikileaks.peer7.de
wikileaks.infinityloop.es
wikileaks.myke.us
wikileaks.jikbag.net
wikileaks.vixns.net
www.kabelspiegel.nl
raubmordkopiert.ws
wikileaks.ludost.net
www.wikileaks.consoled.us
wl.mimamau.de
wikileaks.neofosis.com
www.mistermikileaks.com
wikileaks.antoniojperez.info
wikileaks.ig33k.com
wikileaks.adoutte.com
wl.fuldaecho.de
www.wikileaks-backup.com
wikileaks.bynoob.com
wikileaks.martindv.es
wikileaks.projosh.com
wikileaks.deathserv.net
wikileaks.buckyslan.com
wikileaks.datenwelten.de
wikileaks.samhargreaves.eu
wikileaks.futureoftheinternet.co.uk

wikileaks.jawawa.net
leaks.boerdy.net
wikileaks.trollab.org
wikileaks.k4hosting.com
leaks.underrun.org
wikileaks.tejero.ca
wikileaks.olivu.com
wl.core.am
www.shamanhouse.com
wikileaks.eondream.com
wikileaks.kofuke.org ipv6
dev.quadodo.net
wikileaks.yacy.info
wikileaks.encounterpc.com
wikileaks.spectle.com
whitenetdownloads.com
wikileaks.profithost.net
wikileaks.assaultaddicts.co.nz
wikileaks.holy.jp
www.wikileaks.angelbeast.org
wikileaks.keladi.org
wikileaks.casey-jones.org
wikileaks.permafried.org
wikileaks2.info
wikileaks.openconnector.net
wikileaks.moo2ah.com
wikileaks.blackwire.com
wikileaks-in.ganesh.me
wikileaks.luotettu.net
wikileaks.mahut.sk
wikileaks.plixup.fr
wikileaks.revoleaks.com
www.spacemission.org
wikileaks.hoper.dnsalias.net
wikileaks.tryptamine.net
wikileaks.cancamusa.net
wikileaks.malte.de
wikileaks.gaiadelic.org
wikileaks.persephoneslair.org
wikileaks.styliztique.biz
wikileaks.blokovi.com
wikileaks.lengua.fr
wikileaks.joevr.org
wikileaks.parano.me
wikileaks.picturesbyphilipk.de
wikileaks.renout.nl
wikileaks.hzy.im
wikileaks.adzi.net
wikileaks.wazong.de
wikileaks.redandblack.cz ipv6
wikileaks.erfassungsschutz.net
wikileaks.vyus.de
wikileaks.neurd.org
wikileaks.gundam.eu ipv6
wikileaks.compuspace.nl
wl.i2pbote.net
wikileaks.simleb.cc
www.keepinformationfree.com
wikileaks.jieji.org
wlm.flooble.net
wikileaks.shadowalias.org
wikileaks.goodlifebikes.ca
wikileaks.xr3.cc
wikileaks.lotheac.fi
wikileaks.anarka.nl
wikileaks.data-get.org
wikileaks.hellopal.biz
WL.sanvicentemedia.com
wikileaksmirror.eu
wikiconstitution.info
leaks.no.net
www.wikileaks.angelbeast.org
wikileaks.awardspace.us
wikileaks.pandas.es
wikileaks.mustashwax.com
wikileaks.artwww.net
wikileaks.jordanroy.net
wl.udderweb.com
wikileaks.rlsjrnl.info
janoom.com
wikileaks.xakep.name
wl.davidtyler.we.bs
wikileaks.thebofh.nl ipv6
wikileaks.sw0e.fr
wikileaks.media.pl
wikileaks.escism.net
wikileaks.bacounis.ch
wikileaks.unixnet.dk
wikileaks.is-back.de
wikileaks.nexiom.net
wikileaks.thatfleminggent.com ipv6
www.extremesocial.biz
wikileaks.mooselook.de
wlmirror.riepernet.org
wikileaks.nocworld.com
wikileaks.slite.org
wikileaks.hostingjuice.com
wikileaks.cyberrhea.net
wikileaks.msga.se
wikileaks.505.ru
RealnoeBlinDelo.com
wikileaks.matschbirne.com
wikileaks.aleph-0.net
wikileaks.dugumkume.org
wlmirror.cosego.com
novgorod.zunedevwiki.org ipv6
wikileaks.biz.tm
wikileaks.jadedoto.net
wl.stefanpopp.de
whatever.grillcheeze.com
wikileaks.zakulisa.org
wikileaks.eondream.com
wikileaks.galama.net
wl.newscenterx.de
wikileaks.savetheinter.net ipv6
wikileaks.cybertroops.com
wikileaks.happyforever.com
wikileaks.humanpets.com
wleaks.verymad.net
wikileaks.lotek.org
wikileaks.chronzz.co
wikileaks.tinychan.org
www.rswildy.com
wikileaks.drewhavard.com
wikijm.com
wikileaks.mocek.info
wikileaks.ktula.com
wikileaks.oneeyedman.net
wikileaks.crazzy.se
www2181u.sakura.ne.jp
wikileaked.jamestheawesome.kicks-ass.net
80.70.1.168
wikileaks.jejaring.org
wl2.gernox.de
wikileaks.mine-server.info
bonsainetz.de
wikileaks.imrof.li
wikileaks.lelapinblanc.eu
wikileaks.piratenpartei-nrw.de
wikileaks.skarta.net
wikileaks.radiopark.biz ipv6
wikileaks.labs.fr
wikileaks.matschbirne.com
wikileaks.20.ro
wikileaks.minibofh.org
wikileaks.aamjanata.com
wikileaks.toile-libre.org
wikileaks.zvdk.nl
wikileaks.editia.info
wikileaks.phoeney.de
wikileaks.infotubo.com
www.example.sk
cablegate.savetheinter.net ipv6
wikileaks.aadnoy.no
wikileaks.oliverbaron.com
wikileaks.ladstaetter.at

wikileaks.willjones.eu
wikileaks1.piratenpartij.nl
74.207.247.66
wikileaks.spb.ru
wikileaks.iqaida.de
newark.nj.us.wikileaks-mirror.com
zurich.ch.wikileaks-mirror.com
wikileaks.boneputra.net
wikileaks.csbnet.se
wikileaks.egress.fi
wikileaks.esposium.de
wikileaks.ralforolf.com
wl.farhad.su
wl.it.cx
wikileaks.beispieldomain.org
wikileaks.noreply.to
wikileaks.jejaring.org
gatw.nl
wikileaks.service1.lt
wikileaks.euridies.com
wikileaks.ansible.fr
wikileaks.daphne-dionys.com
wikileaks.beraldoleal.com
wikileaks.trylle.no
wikileaks.nervsoft.com.ar
wikileaks.faked.org ipv6
wikileaks.phpdata.org
wikileaks.sajberhagen.com
wikileak.b1g.nl
wikileaks.goodsoft.lv
wkl.fdumas.fr
wikileaks.byethost31.com
wikileaks.byethost10.com
wikileaks.socketubs.net
wikileaks.sety.cz
beatriceask.se
wikileaks.aditam.org
wlmirror.hopto.org:8000
wikileaks.mazej.net:8080
wikileaks.weis.tk
wikileaks.africanaristocrat.com
wikil.dyndns.org
wikileaks.kor.de
wikileaks.blazor.org
wikileaks.mznshadows.com
cablegate.partidopirata.es
wikileaks.nodehost.co.uk
wikileaks.ihide.in
wikileaks.key-server.de
wikileaks.evilsocket.net
wikileaks.3g.de
wikileaks.b0x.lv
www.mirrorleaks.com
wikileaks.anti-hack.net
wikileaks.ninanoe.net
wikileaks.disi.me
wikileaks.schuijff.com
fremont.ca.us.wikileaks-mirror.com
london.uk.eu.wikileaks-mirror.com
wikileaks.zici.fr
wikileaks.breit.ws
wikileaks.digital-revolution.at
wl.dyndns-wiki.com
wikileaks.finepixonline.de
wikileaks.pancake-pirates.org
wikileaks.goatse.be ipv6
wikileaks.lickmychip.com
wikileaks.topdownmedia.nl
wl.openbotnet.eu
wikileaks.queralt.me
wikileaks.yourhero.de
wl.scottymeuk.co.uk
wl.farhad.su
wikileaks.violetsky.ch
wlmirror.dyndns.org
newfagscanttriforce.com
wikileaks.anthony.lautre.net
wikileaks.facenews.ru
wikileaks.guermonprez.eu
wikileaks.nekochan.ch
wklks.dyndns.org
wikileaks.4574.co.uk
wikileaks.gentlehost.net
wikileaks.knuttinatoll.net
wikileaks.jezustoast.com
wikileaks.wiki-mirror.de
wikileaks.network-13.com
wikileaks.uruknet.com
wikileaks.uenota.org.ua
wikileaks.bitplay.ru
wikileaks.evilhex.org
wikileaks.com.hr
cablegate.technoaddict.fr
wikileaks.walgemoed.net
wikileaks.equal.cluenet.org
wikileaks.sobralhost.com
wl.shathor.com
wikileaks.fuxter.ru
asdf.dhis.org
wikileaks.pod.cvut.cz
wikileaks.nukezone-cnd.com
wikileaks.silenceisdefeat.com
wikileaks.u35.dk
wikileaks.alf0.net
wikileaks.sekil.fr
partyboy.me
wikileaks3.piratenpartij.nl
wikileaks.g0tweb.com
www.wikileaks.udip.hr
wikileaks.venix.eu
wikileaks.version2.nl
dallas.tx.us.wikileaks-mirror.com
wikileaks.tunny.ch
wikileaks.weltgehirnmaschine.de
wikileaks.linuxpro.nl
wikileaks.nijhofnet.nl ipv6
leaks.mooninhabitants.org
innocent-cia-agents.ru
93.90.28.65
wikileaks.kimori.org
wikileaks.webpagearts.com
wikileaks.univers-libre.net
wikileaks.loutre.ch
wikileaks.disruptive.org.uk
wikileaks.interblag.org
wikileaks.jesolo-wants-adsl-back.info
wikileaks.dieinternetprofis.info
whistleblower.futtta.be
wikileaks.xen.no
wikileaks.groissgroissgroiss.com
wikileaks.pub-club.co.uk
wikileaks.orientanet.es
whythenetworks.nl
wikileaks.uenota.org.ua
wikileaks.silverbullion.jp
wikileaks.gonades.org
wikileaks.3xm.es
wikileaks.gvoice.eu
wikileaks.farmavip.net
wikileaks.juiced.nl
wikileaks.brechi.com
cablegate.dev-null.biz
wl.razor1911.com
wikileaks.mserverz.de
wikileaks.bcweb.co.uk
wikileaks.jsphoto.at
wikileaks.michaelkesler.info
wikileaks.bennyjacobs.nl
wikileaks.2114.su
wikileaks.arulns.com
wiki.arrr.tv
wikileaks.synful.us
skaelikiw.kelopez.cl
wikileaks.estlibre.org
wikileaks.reezer.org
wikileaks.felixbecker.name
wikileaks.tbotcotw.com
wikileaks.ebsserver.nl
wikileaks.dashavoo.com

178.77.79.170
wikileaks.av3s.net
leaks.hw.is
wikileaks.brunogola.com.br
wikileaks.gehostet.de
wlm.hor.de
wikileaks.bitmonk.net
wikileaks.espejonegro.org
wikileaks.fahrplan.nl
wikileaks.flurss.com ipv6
wikileaks.propagande.org
wikileaks.karimhossen.fr
wikileaks.tancee.com
wikileaks.kutxa.homeunix.org
wikileaks.scratchbook.ch
wikileaks.bosna-i-hercegovina.info
wikileaks.porkrind.org
wikileaks.obeygravity.de
wikileaks.robsayers.com
wikileaks.mymobile.info
wikileaks.otherreality.net ipv6
wikileaks.maketo.se
wikileaks.varchar.nl
wikileaks.plixup.fr
freedomisimportant.org
wikileaks.delovayakolbasa.ru
wikileaks.islaserver.com
wikileaks.itos.pl
www.leaksmirror.com
www.pucawo.net
wikileaks.hinin.fr
wikileaks.rorbuilder.info
109.109.225.178
wikileaks.sonappart.net
wikileaks.computing-museum.com
wikileaks.dangermouse.ch
wikileaks.spacedigital.eu
www.wikileaks.ma
wikileaks.feh.name
wikileaks.jcowboy.org
wikileaks.sansinteret.info
wikileaks.kaelspencer.com
wikileaks.portalmafia.com
wikileaks.got-root.org
wikileaks.anarchia-networks.com
wikileaks.nodomain.org ipv6
wikileaks.tevatur.com
wikileaks.hunter-9999.de
wikileaks.kewagi.net
www.wikileaks.uk.net
wikileaks.flojpg.info
wikileaks.greenferret.net
wl.minechan.info
wikileaks.runlevel3.org
wikileaks.soft-creation.de
wikileaks.kiney.de
wikileaks.spiltirsdag.dk
wikileaks.dennix.eu
iwikileaks.co.cc
wikileaks.sebastianbartsch.eu
leaks.freecooki.es
wikileaks.justcrashed.net
wikileaks.fauxmerica.com
wl.flan3.net
wikileaks.hlubina.com
wl-tdl.ath.cx
geheimnisse.taegli.ch
wikileaks.extranet.ee
december.freez.in ipv6
wikileaks.mretc.net
wikileaks.co.nl
wikileaks.i-caramba.de
wikileaks.albirar.net
wikileaks.quakeit.de
wikileaks.sharea.tk
wikileaks.fesbi.com
wl.trololol.nl
wleaks.ddsd.de
wikileaks.german-radio.net
wikileaks.tuentichan.org
wikileaks.hackerheaven.org
wikileaks.jugendverein.nl
wikileaks.neodox.org
wikileaks.WhoTheFox.com
vatten.dyndns.org
www.netur.net
wleak.de ipv6
weakylicks.dyndns.org
wikileaks.encoderx.net
wikileaks.vanwoudt.com
wikileaks.ypanema.de
wikileaks.marketmentat.com
leaks.reluctantgrownup.com
1.wl-mirror.eu
wl.crumpledpaper.co.uk
wikileaks.ffwill.homelinux.com
wikileaks.goldendogdev.net
wikileaks.peterelzinga.eu
wikileaks.ilegalniwindows.cz
wikileaks.cs1.ca
wikileaks.pizza-sopranos.nl
wikileaks.wutwhere.net
wikileaks.ste.no
wikileaks.adren.org ipv6
wikileaks.hwsamuel.com
canadapezkiwi.com.ar
wikileaks.txapelbeltz.net
wikileaks.foetusproducts.com
wikileaks.prismation.com
wiki.citizen-cam.de
nepaliwikileaks.org
ewikileaks.co.cc
wikileaks.bodji.net
wikileaks.ecobytes.net
wikileaks.unzane.com ipv6
wikileaks.rolamasao.org
cablegate.dyndns-remote.com
the-loser.net
wikileaks.kermsware.net
www.swisswikileaks.ch
wikileaks.event-lan.net
wikileaks.mein-le.de
wikileaks.uwe.gd
wikileaks.mijniblog.nl
www.wikileaks.rlsjrnl.info
wikileaks.bluug.org
wikileaks.hostalis.net
wkleak.tartiflettes.com
wikileaks.anavallasuiza.com
wikileaks.imrof.li
wikileaks.archive-one.us
wikileaks.rootssh.net
wikileaks.liberal-venezolano.net
wl.paranoidsecurity.nl
wikileaks.redcube.nl
wikileaks.besthost.nl
wikileaks.capitanruby.es
wikileaks.ce.tc
wikileaks2.piratenpartei-nrw.de
wikileaks.insultant.nl ipv6
wikileaks.eldaria.net
wikileaks.dennix.eu
wikileaks.x-tra-designs.org
wikileaks.mindfarming.de
wikileaks.a-dit.fr
wikileaks.diario-geek.com
wikileaks.ilore.de
wikileaks.portalmafia.com
wikileaks.jonateo.com
wikileaks.bluewebdesign.ro
wikileaks.muarf.org
wikileaks.coresec.de
wikileaks.kwain.net
wikileaks.etruhla.cz ipv6
wikileaks.macbay.de
wikileaks.bryanwintermute.com
wikileaks.filteredperception.org
www.wikileaks.enrico-albrecht.de
wikileaks.thatfleminggent.com ipv6

wikileaks.sindro.me
wikileaks.westonwire.com.au
wikileaks.bobotig.fr
wl.bicisxavicano.com
wikileaks.maclupus.net ipv6
wikileaks.sylvie-nicolas.eu
wikileaks2.sytes.net
wikileaks.anidealforliving.com
wikileaks.adactio.com
wl.shiftcontrol.org ipv6
wikileaks.hechocomoelorto.com.ar
wikileaks.thefrogz.net
wikileaks.sharegroundz.com
wikileaks.leet.la
wikileaks.isaaccastro.eu
wiki-leaks.org.ua
wlm.wealthfare.org
wikileaks.vervloekt.nl
www.wikileaks.exclusive-consulting.info
wikileaks.gibraine.com
www.yeswecat.es
wikileaks.ldmf.ch
wikileaks.riot-act.org
wl.deleteme.fr
wikileaks.natrox.org
www.wikileaks.rlsjrnl.info
wikileaks.markliveshere.com
wikileakspr.com
wikileaks.miro.ir
wikileaks.prowikileaks.com
www.wikileaks.ulagatamiloli.com
wikileaks.exclusivenet.cz ipv6
wikileaks.t-muh.de
wikileaks.xrz.tw
wikileaks.chaosberlin.de
wikileaks.mattdm.com
wikileaks.kex3.com
wikileaks.bachkhoathu.com
wikileaks.relaxman.nl
wikileaks.oma-kollegiet.dk
wikileaks.secretweb.at
wikileaks.0o.cz
wikileaks.zioinc.com
wklks.robertogabrielli.net
87.106.248.5
wikileaks.chrisbrandt.de
wikileaks.bluuurgh.com ipv6
wikileaks.matthijs.at
wikileaks.exclusivenet.cz ipv6
wikileaks.anoluz.net
wikileaks.letolier.net
wikileaks.ozazar.org
wikileaks.gnog.ch
wikileaks.gecko.tc
wikileaks.kunfoo.org
wikileaks.miopiapolitica.mx
wikileaks.warrantyvoid.de
wikileaks.haaparanta.se
wikileaks.abadcer.com
wikileaks.realitysink.com
wikileaks.greva.ro
wikileaks.sansinteret.info
wikileaks.it.cx
wl.kofuke.org ipv6
wikileaks.extme.eu
start.hating.us
wikileaks.tepames.net
wikileaks.graafschap-online.nl
x-file.com.ar
3210.dyndns.biz
wikileaks.megahuge.com
wikileaks.huisjesmelkers.nl
wikileaks.wiglaf.net
wikileaks.theawayteam.org
wikileaks.arenyestratosferic.info
wikileaks.socialismsocialismsocialism.or...
cg.antalyaadrasan.com
72.14.189.17
leaksmirror.com
wikileaks.csjk.de
wikileaks.deigualaigual.net
wikileaks.epicwinrar.com
www.wikileaks.rlsjrnl.info
wikileaks.panthera.ro
www.helpwikileaks.co.za
wikileaks.robertpenner.com
wikileaks.anduin.net
wikileaks.philoucorp.fr
wikileaks.computing-museum.com
www.cns-systems.de
wikileaks.unrforliberty.com
wikileaks.tuxonauten.de
leakswiki.dyndns.info
wiki.abcd1234.de
rsf.co
wikileaks.voima.fi
leaksasylum.dyndns-wiki.com
wl.reto-schneider.ch
wikileaks.passion4rock.com
wikileaks.theapplefarm.net
wl.canya.net
wikileaks.buffer.dk
wikileaks.whatevz.net ipv6
wl.batu.me
wikileaks.2lm.de
wikileaks.kinderporno.cz ipv6
wikileaks.tachanka.org
wikileaks.amakiir.net
wikileaks.warperbbs.de
wikileaks.d-hc.ru
wikileaks.home-land-security.info
wikileaks.mediabrief.nl
wikileaks.dupnet.org
leakz.dyndns-server.com
wikileaks.sjmulder.nl
wleaks.dyndns.info
wikileaks.non-self-descriptive.org
wikileaks.lorea.org
wl.uberism.net
wikileaks.therabithole.org
wikileaks.guidomgs.com.ar
wikileaks.dusse.fr
wikileaks.evermeet.eu
wikileaks.unibrennt.at
wikileaks.gedankenverbrechen.org
wikileaks.epter.com
wikileaks.marketmentat.com
wikileaks.tepames.net
wikileaks.isecharlotte.com
www.savetheleaks.org
wikileaks.seotaurus.com
wikileaks.trollocracy.com
213.133.123.117
v795.vir.kagoya.net
wikileaks.zdark.com
wikileaks.frontlawn.net
freedom.fortworthlocksmiths.com
wikileaks.1777.fr ipv6
wikileaks.hmfaysalconnect.com
wikileaks.olywip.org
wikileaks.openstreetmap.pl
wikileaks.flojpg.info
wikileaks.libriste.net
wikileaks.chillers-media.com
wikileaks.glennie.fr
wikileaks.netzistenzminimum.de
wikileaks.gormotte.info ipv6
wikileaks.majinboo.org
wikileaks.hac.cc
wikileaks.7dots.de
wikileaks.bosna-i-hercegovina.info
wikileaks.chormeos.com
wikileaks.domainfactory-kunde.de
wikileaks.overt-ops.net
188.94.113.24
wikileaks.red-net.info ipv6
wikileaks.bluewebdesign.ro
www.wleaks.nl
wikileaks.nonews.net

wikileaks.la-gauche-vsr.ch
wikileaks.1o5.ch
wikileaks.azylum.org
wikileaks.fisquimia.es
174.142.5.19
wl.mryoichi.com
wikileaks.elpatibulo.es
wikileaks.lapampafestival.de
wikileaks.yaki-syndicate.de
wikileaks.tarikin.com
wikileaks.accessoriesdirect.co.nz
wikileaks.kokev21.com
wikileaks.fayatux.me
wikileaks.obikenobi.eu
wikileaks.liberdadedeexpressao.net
wikileaks.skyhost.bg
wikileaks.olsc.org
wl.qwuh.com
wikileaks.thomas-weinbrenner.de
wikileaks.2smart4u.de
wikileaks.iptunnel.de
wikileaks.freetekno.nl
wikileaks.insultconsult.net ipv6
wikileaks.stekkz.com
wikileaks.orilla.de
wikileaks.lunatic-asylum.eu ipv6
wikileaks.kyak106.com
wikileaks.sisepudo.com.mx
wikileaks.rutton.org
wikileaks.filesplit.us
wikileaks.piratskapartija.com
wl.enneu.net ipv6
wl.8mm.cc
wikileaks.nachrichtenradio.eu
www.wikileaks-germany.de
wikileaks.2gi.de
wikileaks.dajla.org
wikileaks.barabel.net
wikileaks.mantrain.me
wikileaks.thalmannsoftware.com
wikileaks.solidfiles.org
wikileaks.l3b.de
wikileaks.knifeprty.net
wlmirror.muehlbachler.org
wikileaks.kklasen.net ipv6
wikileaks.strycore.com
wikileaks5.no-ip.org
wikileaks.vanleuven.org ipv6
wikileaks.it.ca
wikileaks.nodo50.info
wikileaks.tx-0.org
wikileaks.prof-maad.org
wikileaks.bastok.nl
wikileaks.mosheff.ru
wikileaks.freekynet.de
wikileaks.shtuchki.biz
wikileaks.gr-ivanov.com
wikileaks.systemelibre.fr
wikileaks.acidmonkey.cz
wikileaks.bilderbergips.org ipv6
wikileaks.obeygravity.de
wikileaks.hausbergadler.de
wikileaks.trsi.org
xgfx.ch
www.janoom.com
leaked.dyndns.org
wikileaks.googme.eu
www.wikileaks.imaginaction.eu
wikileaks.sharegroundz.com
wikileaks.holy.jp
www.beertology.org
wikileaks.softplaces.net
wikileaks.ppuk.me.uk
64.191.45.85
wikileaks.svhpu.net
wi.kileaks.net
wikileaks.valerauko.net
wl.t0g.de
wikileaks.qgm.com
leak.thehackersedge.com
wikileaks.gpljihad.org
wikileaks.sfany.com
wikileaks.enfranchisedmind.com
www.nachtploeg.eu
wikileaks.piratupartija.lt
wikileaks.frnxs.net
lksmrrr.dyndns-wiki.com
wikileaks.spikex.homelinux.net
wikileaks.goliath.nl
wikileaks.graficautopica.net
wikileaks.ranta.ch
wikileaks.geheimdienste.de
wikileaks.gwolf.org
wurst.nl
wikileaks.thebuble.org
wikileaks.beneth.fr ipv6
cables.padonma.com
wikileaks.bryanfarmer.com
wikileaks.sukria.net
gg.burble.de
wikileaks.artemisanet.com
wikileaks.bigini.net
wikileaks.dagams.de
wikileaks.kowalski-clan.de
wikileaks.nucleartesuji.com
wikileaks.makat.org
www.wikilekje.nl
wikileaks.peelo.net
wikileaks.darkmoon-studio.com
wikileaks.dwmobil.de
wikileaks.xdel.ru
www.wikileaks.adzi.net
wikileaks.toposerver.es
wikileaks.greate.st
wikileaks.bernhardluginbuehl.ch
wikileaks.das-quaddy.de
wikileaks.antisnatchor.com
wikileaks.xek.pl
wikileaks.bytopia.dk ipv6
wikileaks.lentas.org
wikileaks.osbg.at
wikileaks.viscom3.com
wikileaks.lotheac.fi
wikileaks.euskogeeks.com
www.wikileaks.transparency.uni5.net
wikileaks.alienclub.ro
www.wikileaks.waaromis.nl
mirrorleaks.org
wikileaks.xiala.net
wikileaks.escape-to-space.com
wikileaks.ak-online.be ipv6
wikileaks.ushare.nl
cablegates.dyndns.org
wikileaks.0st.org ipv6
wikileaks.server-king.de ipv6
wikileaks.mylawforall.com
wikileaks.lobotomie.org
wikileaks.os3.nl ipv6
cablegate.hunko.eu
wikileaks.albavence.com
wikileaks.1200wd.com
wikileaks.srsly-aweso.me
wikileaks.komodin.org
wikileaks.jcserver.net
wikileaks.yassinetrabelsi.com
wikileaks.silke.in
wikileaks.jaguarhost.com.br
wikileaks.vanoeffelhaarlem.nl
wikileaks.entrecartones.com
wikileaks.iamjulianassange.com
www.norbiman.com
wikileaks.x1598.at
wikileaks.tachanka.org
wikileaks.j0hnx3r.org
wikileaks.ilostmyself.org
honestgovernment.org.uk
wlmirror.co.uk
wikileaks.insecurenet.info
wikileaks.bonzer.it

fallingleaves.dyndns.org
www.wikileaks.samp-online.com
wikileaks.the-luckyduck.de
wikileaks.gardmo.se
thetruth.dyndns.info
www.bsinfotech.net
wl.r15.ch
wikileaks.notsocomplicated.org
badeio.wleak.de
wikileaks.mitov.eu
wikileaks.akegata.se
wikileaks.gzmod.com
deletia.org
wikileaks.sebastianehinger.de
wikileaks.hacklabvalls.org
wikileaks.trollab.org
wikileaks2.piratenpartei-nrw.de
wikileaks.jedinerd.net
wikileaks.goldrunner.de
wikileaks.borntobooze.com
wikileaks.emi-area.com
wikileaks.orientedhosting.com
wikileaks.opensomething.org
wikileaks.dewereldmorgen.be
cachee.net
wikileaks.thefrogz.net
wikileaks.revreso.de
wikileaksmirror.anarchisthosting.com
wikileaks.yeeve.de
wikilleaks.dyndns.biz
wikileaks.redfoxcenter.org
wikileaks.vinzei.com ipv6
wikileaks.spacemoo.net
wikileaks.velotype.nl
wikileaks.deicio.net
wikileaks.pepzi.org
wikileaks.kollau.nl
wikileaks.etv.cx ipv6
173.52.107.78
wikileaks.pato.org.mx
wikileaks.frankkalana.com
wikileaks.adminctrl.com
wikileaks.eaclan.net
wl.jonnyscholes.com
wikileaks.triggerdesign.yourweb.de
last.to
wikileaks.belfalas.org
wikileaks.mladina.si
wikileaks.47chan.net
wikileaks.dieflieger.net
wikileaks.aspektratio.net
wikileaks.dyndns-work.com
wl.saymonz.net
wikileaks.hunstus.de
wikileaks.whitescreen.se
wikileaks.server0.eu
wikileaks.tux-ie.nl
wikileaks.dabax.net
wikileaks.gpssrbija.com
wikileaks.infinitemedia.nl
wikileaks.deca.cat
wikileaks.last-straw.net
wikileaks.sshbl.eu
wikileaks.maidireradiomaria.com
wikileaks.drumandbass.lv ipv6
wikileaks.xsicht.me
wikileaks.securebydesign.nl
wikileaks.aussieitguy.com
wikileaks.xchatfr.org
wikileaks.atreides.ch
wikileaks.glitteringplain.net
wikileaks.goldrunner.de
wikileaks.kister.org
wikileaks.thehash.es
cablegate-mirror.dyndns.biz
outpost.fluxzone.net
www.wikileaks.yopo.es
wikileaks.palisades-berlin.de
wikileaks.equiv.se
wikileaks.blue-style.info
wikileaks.tuxamito.com
wikileaks.lsncdn.net
wikileaks.cloudyks.org
wikileaks.flax-town.se
wikileaks.instropy.com
wikileaks.eklind.org
wikileaks.fam-debray.de
wikileaks.truthispornography.com
wikileaks.telesletjes.be
wikileaks.robertpenner.com
wikileaks.cluster.nu
wikileaks.pounce.org ipv6
wikileaks.dwtn.to
leaks.communitywerkstatt.com
wikileaks.themojave.com
wikileaks.northernsamizdat.ca
wikileaks.blogator.de
wl-tdl.ath.cx
wikileaks.dpate.com
wikileaks.plentyfact.org
wikileaks.unit2.ca
www.wieselbau.net
wl.drecksserver.de
wikileaks.pnuke.de
wikileaks.inter.net.my
wikileaks.thfakenick.net
wleaks.dyndns.biz
wikileaks.umatrail.org
wikileaks.zoolink.com
wlmirror.info
wikileaks.100gartenzwerge.de
wikileaks.pkol.de
wikileaks.podgorny.cz
wikileaks.seaconflict.com
wl.z4k.de
wikileaks.baarda.org
imaginaction.eu
wikileaks.egroc.de
irritant.org.uk
wikileaks.helvetet.com ipv6
wikileaks.intresseklubben.org
46.4.203.216
wikileaks.not-on.com
wikileaks.die-lega.org
wikileaks.anti.ch
wikileaks.plebis.net
wikileaks.marty.co
wikileaks.lenselink.biz
wikileaks.italy.indymedia.org
www.wikileaks.17thad.de
www.mirror.ch0.in
wikileaks.pvane.com
wikileaks.shneeble.com
wikileaks.liberale.at
wikileaks.gnuab.org
wikileaks.dan.ec
wikileaks.liberdadedeexpressao.net
wikileaks.jollymushr0om.de
wiki.leaks.org.in ipv6
douze-bis.net
wikileaks.fuckitall.nl
wikileaks3.info
wikileaks.frozenhydro.com
wl.yaskulka.net
wikileakage.dyndns.org
wikileaks.qgm.com
wikileaks.werpo.com.ar
wikileaks.sinsordina.cl
wikileaks.dennismueller.eu
wikileaks.ip-rebel.ch
wl.lighthomebd.com
wikileaks.kartonnet.co.cc
www.wikileaks.acontrario.org
wikil3aks.info
jswleaks.for-our.info
wikileaks.radnode.com
wikileaks.505.ru
wikileaks.jbfavre.im ipv6
wikileaks.zworski.com

wikileaks.indrekpaas.com
wikileaks.martystrong.co.uk
wikileaks.jan-deluxe.de
wikileaks.coderzplaza.com
wikileaks.otakuturk.com
www.wikileaks.infohs.com.br
a6k.dyndns.org:80
wikileaks.thorx.net
wikileaks.machinaesupremacy.com
wikileaks.ftp.sh
wikileaks.skriveleif.com
wikileaks.cyberarmy.at
wikileaks.oikos.paneidos.net
wikileaks.chalgabox.com
wikileaks.nosgaming.com
leaked.no-ip.org
wikileaks.xtreme-faulpelz.de
wikileaks.yankovsky.me
wikileaks.christiansson.net
wikileaks.servicetorrent.com
chto.info
mirrorleak.org
wikileaks.adeut.es
wiki.kiwiculture.de
wikileaks.wackazong.com
wikileaks.1upload.de
wikileaks.thingee.net
leaks.rheincoach.de
wikileaks.org.rs
wikileaks.dysth.com
wikileaks.ywettka.sk
wikileaks.dealicanteajapon.com
wikileaks.dennusb.nl
wikileaks.pcte.ch
wikileaks.31337.be
wikileaks.hfbk-hamburg.de
wikileaks.enlaondatv.com
wikileaks.malayalarajyam.com
www.wikileaks.die-nachdenker.de
wikileaks.adinox.ch
leaked.no-ip.info
88.198.169.6
wikileaks.robintel.org
wikileaks.vjultra.co.uk
wikileaks.scarabel.es
wikileaks.andalucialibre.es
wikileaks.j1b.net
wikileaks.biffer.de
server2.wlmirror.co.uk
wlmk.dyndns.info
wikileaks.ppuk.me.uk
wikileaks.kabo.nu
wikileaks.yampe.com
www.aboutislamabad.com
wikileaks.quesaben.org
mirror-wikileaks.de
wikianon12.pcriot.com
wikileaks.basilisksolutions.com
wikileaks.seotaurus.com
wikileaks.fuckedup.cc
wikileaks.adseen.de
wikileaks.dersonic.org
wikileaks.zdravo.com.mk
wikileaks.kimeru.org
wikileaks.6m.se
www.wikileaks-mirror.at
leaked.dyndns.info
wikileaks.morphy.info
www.wikileaks.antisys.com
wikileaks.vn.ua
www.wikileakspower.nl
wikileaks.blackforgestudios.com
www.markmccoy.org
wikileaks.jofonet.net
wikileaks.cyberarmy.at
wikileaks.nischi.ch
wikileaks.zdravo.com.mk
wikileaks.nickileaks.com
wikileaks.url-indexer.com
wikileaks.aigul.com
wikileaks.untrusted.de
wikileaks.olbion.com
81-89-103-142.blue.kundencontroller.de
wikileaks.arza.us
wikileaks.hjsnetworks.net
wikileaks.klockenstein.se
wiki.leaks.li
wikileaks.gh05tn3t.net
wikileaks.happypuppies.net ipv6
wikileaks.flamer-scene.com
wikileaks.evergreenterrace.de
wikileaks.bloodyweb.com
wikileaks.energize.cc
wikileaks.jan-deluxe.de
wikileaks.datensaaten.de
wikileaks.podc-aster.nl
wikileaks.my-niap.org
wikileaks.dvonline.co.uk
wikileaks.vakarazinas.lv
wikileaks.cbin.pp.ua
wl.g7s.org
wikileaks.bremenleaks.de
wikileaks.bufta.ch
www.dogta.at
wikileaks.khemael.net
wl.kh.ro
wikileaks.matsta.de
freiheit.ihlowerhoern.de
wikileaks.andygo1.de
wikilix.meilard.fr
wl.nul343.nl
wikileaks.codeblue.uk.to
wikileaks.org.mx
leaksmirror.dyndns.org
wikileaks.zigg.me
wikileaks.outofbounds.nl
wl.helden-der-freiheit.de
wikleaks.co.cc
wikileaks.freiescientologen.de
wikileaks.c0mhost.net
178.49.28.209
wikileaks.kechel.de
wikileaks.ubs.ath.cx
wikileaks.partner.md
wikileaks.pixur.se
wl.freecandy.org
wikileaks.therabithole.org
wikileaks.waelelebrashy.com
wikileaks.adactio.com
wl.dasserver.com
wikileaks.jboettger.de
wikileaks.anendhasastart.eu
freedom.fortworthlocksmiths.com
wikileaks.tweakenl.info
wikileaks.w4m.at ipv6
freedom.fortworthlocksmiths.com
wikileaks.killy.me
wikileaks.maroxrickshaw.com
wikileaks.volksfestplatte.de
wikileaks.halogalaxy.eu
www.wikileaks-mirror.dk
wikileaks.dss-bs.de
wikileaks.hacktivistas.net
www.g-zero.net
wikileaks.zebo.co.nz
wikileaks.hit-repeat.net
wikileaks.rogierbeckers.com
wikileaks.simoncoetzee.com
wikileaks.oscarcillo.com
wikileaks.one-true.net
wikileaks.dragora.net
www.wikileaks.eitorf-online.com
bielawa.freecast.pl
wikileaks.datensaaten.de
wikileaks.kirashi.ca
wikileaks.hostatic.ro
wikileaks.pe
wikileaks.nerdevice.com.mx
wikileaks.brunz.ch

wikileaks.korwin.tv
wikileaks.lez.name
youmaystopthisindividualbutyoucantstopus...
wikileaks.jemag.nl
wikileaks.phillysaxon.net
wikileaks.koulen.org
wikileaks.democratuur.nl
wl.hetdupke.nl
wikileaks.dead7.de
wikileaks.metanormal.de
wikileaks.bjornju.nl
home.brandl.net
sinde.melaco.me
wikileaks.wof1037.be
wikileaks.levelhost.com.br
wikileaks.fsinf.at
wikileaks.alterzine.fr
wikileaks.kotuha.info
wikileaks.jerome.cc
wikileaks.sacnr.com
wl.salemlongboarding.org
wikileaks.depthsofmuc.com
wikileaks.dunck.us
wikileaks.wargam.es
wikileaks.unrforliberty.com
wikileaks.200g.org
wikileaks.eichruss.ch
wikileaks.netfreak.ca
wikileaks.patrickkivits.com
wkl01.jieji.org
wikileaks.caffeinator.net
wikileaks.andservicesforall.com
wikileaks.dragosgaftoneanu.com
wikileaks.mosmo.de
wl.nl1.tern.org.nz
wikileaks.deb-support.de
wikileaks.motociclonfo.it
wikileaks.redkloud.net
stillalive.ehf-team.es
wikileaks.linuxmce.org
wiki.leaks.es
wikileaks.s1cness.com
wikileaks.whitet.net
wikileaks.bloodredskies.org
wikileaks.3trust.com
wiki.ga-college.org
wikileaks.matej.tk
wikileaks.pakkianathans.com
wikileaks.dedonacara.com.br
207.150.191.187
text.dyndns.tv
wikileaks.l0cal.com ipv6
wikileaks.teamslack.net
wikileaks.planet.ee
aspaleaks.dyndns.org
wikileaks.bartworx.de
wikileaks.nowak2000.de
wookieleaks.org.uk
mirrorwiki.dyndns.org
wikileaks.mahtisoturit.net
wikileaks.cmantito.com
wikileaks.berrysds.org
wikileaks.mahtisoturit.net
wikileaks.flashdance.cx ipv6
wikileaks.linux-101.org
wikileaks.twin-towers-down.de
wikileaksrussia.ru
wikileaks.gagniard.org
wikileaks.antikapitalistische-linke.de
wikileaks.iamkura.com
wikileaks.retrojogos.org
wikileaks.gotaweb.com.br
wikileaks.lunattidesign.com
wikileaks.okhosting.com
wikigeneration.org
dasboot.dyndns.tv
wikileak8657.dyndns.org
section9.twilightparadox.com
leaks.manurevah.com
wikileaks.skepie.nl
wikileaks.starapple.nl
wikileaks.cyrtophora.com
soviet.jp
wikileaks.blogofsysadmins.com
cablegate.partidopirata.es
wikileaks.casimir1904.com
wikileaks.bubele-server.de
wikileaks.kbdw.net
wikileaks.civvic.ro
wikileaks.tecnocaina.net
www.1wise.es
wikileaks.puddipuddi.ch
wikileaks.dabeed.net
wikileaks.4-eachother.net
wikileaks.s1cness.com
wikileaks.bacounis.ch
wikileaksmirror2010.tk
92.233.200.186
wikileaks.voxelperfect.net
www.ragnabattle.com
wikileaks.againstthesystem.com
wl.nische4.com
wikileaks.dirkeinecke.de
wikileaks.holam.hk ipv6
wikileaks.exion.ch
wikileaks.qrios.de
www.jtf.at
wikileaks.codejungle.org
wikileaks.persephoneslair.org
wikileaks.andreas-skoglund.se
wikileaks.annawajda.com
wikileaks.robinhuitenga.nl
wikileaks.spywarelan.se
www.wikileaks.rimeallaf.com
wikileaks.pirates.ie
www.ikkeleaks.com
wikileaks.da.ru
www.teem.it
wikileaks.xiante.com
wikileaks.tomcisar.at
wikileaks.blueglowy.com
wikileaks.my-xaub9r.de
wikileaks.ok1.ca
praetorian.dynalias.net
wl.errenovenove.net
wikileaks.vntx.net ipv6
w.liansi.org
wikileaks.ithic.com
wikileaks.xn--fdr45z90g374a.jp
wikileaks.prevalent.de
wikileaks.rez0r.info
wkl.alcatros.net
wikileaks.level-10.de
wikileaks.jordielferink.tk
wikileaks.skatalites.net
wikileaks.trfl0r.de
wikileaks.oark.org
wikileaks.project-serenity.be
wikiliks.ehrepli.mine.nu
wikileaks.guilde-amaterasu.org
wikileaks.imaginaction.eu
wikileaks.mbcg.se
wikileaks.yabc-clan.de
wikileaks.grids.be ipv6
wikileaks.lair.cc
wikileaks.function.io
wikileaks.evoluve.info
wikileaks.cmantito.com
wikileaks.urpedia.org
wiki.aitn.co.uk
www.wikileaks.za.org
213.165.84.77
wikileaks.vitorfernandes.org
wikileaks.exi5tenz.net
wikileaks.brauchen.info ipv6
wikileaks.100x100.lt
wikileaks.commanders.ch
www.wikileaks.xe1jeg.com
wikihelp.tugatech.com.pt

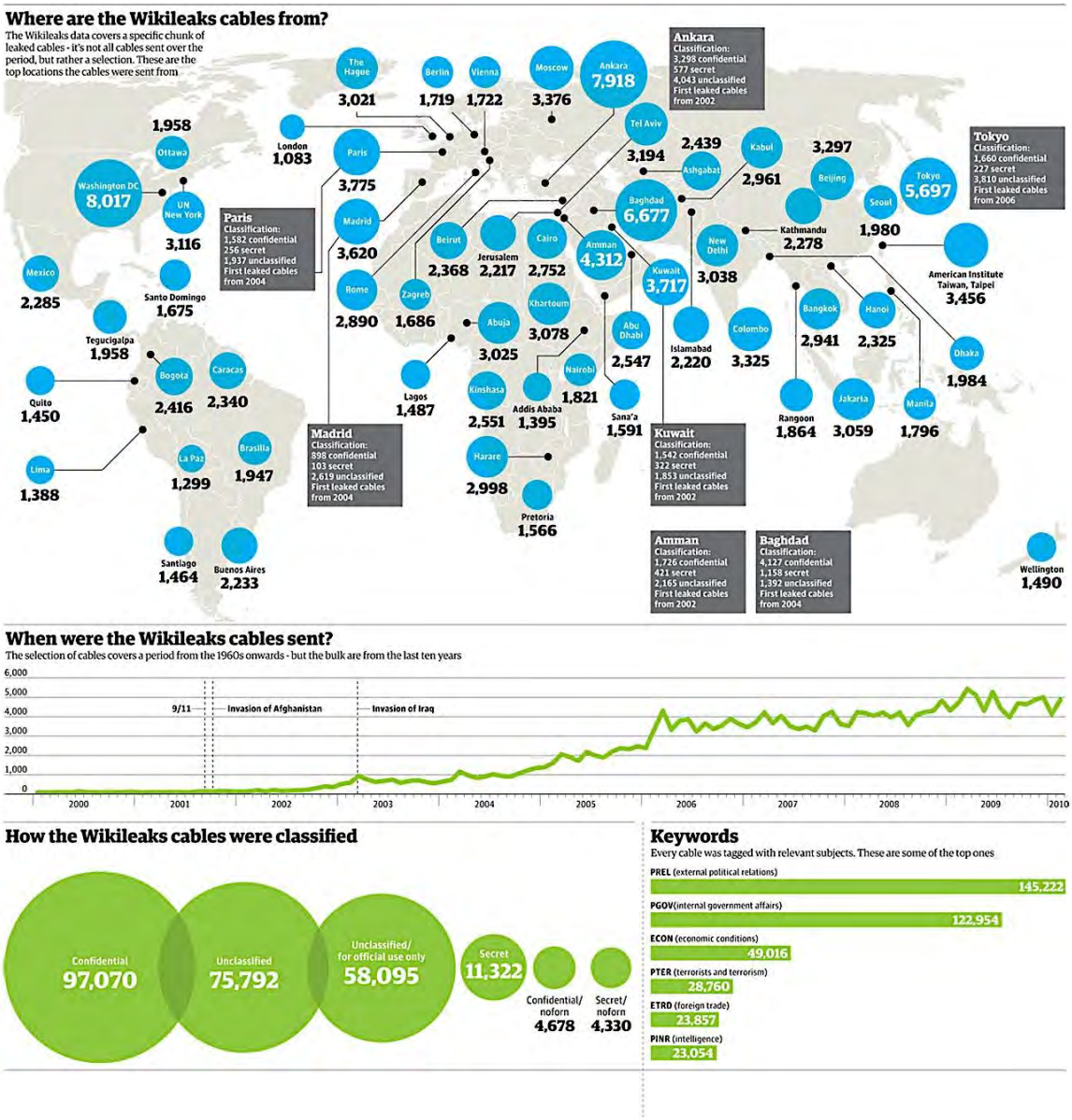
wikileaks.hostmauher.com.ar
wikileaks.wof1037.be
wikileaks.sugarheadfest.org
wikileaks.delfic.org ipv6
wikileaks.geizhals.org
www.brooklynsbestburgers.com
wikileaks.lifeware.ru
wikileaks.sizoberz.de
wlm.gpuimpulsereverb.de
wikileaks.dayscholars.com
wikileaks.willist.com
soviet.jp
www.wikilek.net
wikileaks.rilla.es
wikileaks.cglobe.ru
www.giswald.de
www.giswald.de
wikileaks2.cz.cc
wikileaks.lif.at
wikileaks.njofra.net
wikileaks.ulteemate.com
wikileaks.jdubshub.com
wikileaks.essedici.no-ip.org
wikileaks.levelcap.net
www.all-import.de
wikileaks.barrabin.org
wikileaks.stusplace.net
wikileaks.fanatic.be
gchq.eu
wikileaks.pignouf.fr ipv6
wikileaks.enciclopedia.com.pt
wl.icicleinacubicle.com
www.wikile4ks.de
wiki.x0r.su
bieber.lt
wikileaks.estadolateral.net
wikileaks.themarthachronicles.com
wikileaks.barakotta.com
wikileaks.kabelsearch.org ipv6
wikileaks.insurgen.cc
wikileaks.bordeelsletjes.nl
wikileaks.mouafik.fr
emeraldviewer.sl
wikileaks.trystopus.org
wikileaks.rendas.cz ipv6
wikileaks.moon-station.us
wikileaks.axdf.net
wikileaks.prevalent-digest.de
wikileaks.seckupeter.ch
wikileaks.pure64.net
wl.asanebo.net
wikileaks.beme-it.de
wikileaks.siliconpoetry.com
wikileaks.xnv.nl
www.wikileaks.paraflipar.es
wikileaks.name-service.de
wikileaks.cesarvalencia.ws
wikileaks.reichsoverheid.nl
wikileaks-mirror.zihoster.com
w1k1leaks.dyndns.org
parsley.student.utwente.nl
wikileaks.openhackers.tk
wikileaks.tydirium.nl
wikileaks.rymdlego.se
wikileaks.dokterbob.net ipv6
wikileaks.d2k5.com
www.estou.in
91.192.100.156
wikileaks.osk4.cz
wl.bananarocker.org
wikileaks.mindhack.at
wikileaks.hashbang.ca
wikileaks.faderpc.com
wikileaks.vahue.org
wikileaks.xatrix.org
wikileaks.vipperland.com
france.copyleaks.org
wikileaks.sportsload.cc
www.cablegate.me.uk
wklks.aphru.org
shylux.dyndns.org
wikileaks.kode.co.za
wikileaks.demmserve.co.cc
wikiservers.net
www.wleaks.es
wikileaks.zipman.it ipv6
wikileaks.xboxplayer.net
www.leakywiki.org
wikileaks.netzrasen.de
wikileaks.retro-hosting.co.uk
wikileaks.nuac.org.au
wikileaks.pparth.org
wikileaks.blindmanstudio.com
wikileaks.fitfeed.co.uk
wikileaks.dreamhosters.com
leakypipe.moregeneric.com
wikileaks.colinaroja.org
wikileaks.marpeck.net
wikileaks.gmards.com
www.tydirium.nl
Wikileaks.botnet.co
www.wikilek.net
wikileaks.sileht.net
wikileaks.giwah.it
wikileaks.blumirror.de
wikileaks.yopui.com
wikileaks.hdscript.de
wikileaks.estou.in
wl.monkeybit.net
wikileaks.iolardemartini.com.br
wikileaks.star-nova.eu
wikileaks.frank-sierra.com
wikileaks.freehostia.com
wkleakschile.hellbringers.cl
wikileaks.ffwill.homelinux.com
wikileaks.sativouf.net
the-nobody.de
wikileaks.the-nobody.de
www.truthwillwin.net
wikileaks.khan.su
wikileaks.doublemarked.com
wikileaks.n3t5ky.nl
wikileaks.sileht.net
wikileaks.odiando.com
wikileaks.bardoul.nl
wikileaks.govnorg.ru
wikileaks.stableserver.ru
wikileaks.tiifp.org
wikileaks.bobop.co.uk
wikileaks.noiseandheat.com
www.all-import.de
www.leaksmirror.com
wikileaks.hochstaetter.info ipv6
wikileaks.tensor.gdynia.pl
wl.kotlovnica.si
wikileaks.wikrati.se
wikileaks.ateneuabril.org
wikileaks.scribbls.net
wikileaks.disi.me
newworld.mooo.com
wikileaks.ivanoel.net
wikileaks.0st.fr
cablegate.student.utwente.nl
leaks.nadazero.net
wikileaks.v30x.net
wikileaks.cinestecia.com
wikileaks.cleverhosting.co.uk
wikileaks.webapse.com
leakypipe.moregeneric.com
wikileaks.rendas.cz ipv6
wikileaks.criticapura.com
wikileaks.theoriginals.in
wikileaks.gohost.cz
sukciai.lt
wikileaks.rberet.com
www.meineleaks.net
wikileaks.su.no
wl.davy.net.au
wikileaks.journalisten.no

wikileaks.ethictoc.org
wikileaks.init-0.net
wikileaks.dutchan.org
wikileaks.tralala.cz.cc
wikileaks.onyxias.com
wikileaks.q23p.de
wikileaks.dontassrape.us
wikileaks.grupoexis.es
wikileaks.jachenau-tetra.de
wikileaks.ictrocks.nl
wikileaks.goainfected.me
wleaks.org.ua
wikileaks.porkrind.org
wikileaks.star88.de
wikileaks.tomerikstower.com
wikileaks.21designs.co.uk
wikileaks.insidenothing.com
wikileaks.andrewboring.com
wikileaks.flatworld.eu
wikileaks.felipecypriano.com
220.233.65.211
wikileaks.gruene-linke.de
wikileaks.figaronron.com
wikileaks.privacyisdood.nl
wikileaks.netzarea.de
yoxx.dyndns.org
wikileaks.fierman.info
wikileaks.matej.tk
wikileaks.linitch.nl
wl.rhythmsofresistance.co.uk
wikileaks.recursiva.org
wikileaks.ideologic.ws
wikileaks.c0ws4y.com
wikileaks.noppo.nl
wikileaks.13x37.net
wiki.hooyandex.com
wikileaks.maarstreetboyz.org
wikimee.info
wikileaks.idealogic.info
wikileaks.alf0.net
wikileaks.postrmagazine.com
wikileaks.bsdmp.org
wl.iceatronic.net
wikileaks.shatteredmods.com
wikileaks.opusnotion.com
wikileaks.server-mdm.x10.bz
wikileaks.flamesong.com
wikileaks.the-sps.org
wikileaks.medienkueche.info
wikileaks.poah.net
wikileaks.xf.cz
wikileaks3.dyndns.org
wikileaks.adna.de
wikileaksmirror81.no-ip.org
3u.ro
www.dutchwikileaksmirror.nl
wikileaks.liberation.fr
wikileaks.kubinformatique.fr
wikileaks.neveleno.ru
wikileaks.zavinagi.org
wikileaks.allmarkedup.com
wikileaks.prometheus.ie
wikileaks.oztivity.com
wikileaks.morphy.info
wikileaks.rhnz.eu
www.wikileaks.triciakennedy.com.au
wikileaks.live-on-stars.de
wikileaks.mine.sk
wikileaks.itespresso.net
wikileaks.crome.us
wikileaks.mcdinner.de
wikileaks.movimentacaoucs.com.br
wikileaks.zoolink.com
wikileaks.baryon.net
wikileaks.softgen.ge
wikileaks.stacktrace.nl
wikileaks.robkaper.nl
wikileaks.gaf.at
wikileaks.kevzan.net
wikileaks.pandacreation.fr
wikileaks.dl1mnu.de
wikileaks.chezseb.net
wikileaks.iolardemartini.com.br
wikileaks.pachafoundation.org
wikileaks.roestertaube.de
www.wikileaks.millenares.net
gchq.eu
69.73.172.85
wikileaks.citizen-k.net
wikileaks.indrekpaas.com
wikileaks.enkore.de
wikileaks.newworldorder.de
wikileaks.computer42.org
wikileaks.punchenko.ru
wikileaks.rengiared.com
wl.175.at
wikileaksp.ublica.com
wikileaks.stedelijkwonen.net
web.lightpath.ca
wikileaks.blogator.de
www.wikileaks.l7media.de
wikileaks.kisai.info
wikileaks.research-labs.net
wikileaks.scoffoni.net
wikileaks.micaroni.org:8080
wikileaks.newzbin.com
wikileaks.robkaper.nl
wikileaks.phelix.lv
wikileaks.schnypsel.de
wikileaks.kubinformatique.fr
wikileaks.tyruiop.org
wikileaks.dp.ru
wikileaks.wetterpirat.de
wikileaks.qedx.com
wikileaks.nebelfetzen.de
wikileaks.xt.pl
w.liansi.org
wikileaks.webshox.org
wikileaks.liveproject.eu
www.wikileaks.rlsjrnl.info
wikileaks.rubrikk.no
wikileaks.planetame.com
www.wikibullshits.org
wikileaks.it-kartellet.dk
wikileaks.raymondhill.net
wl.goldencondor.org
wikileaks.jordanielalves.com.br
wikileaks.marsho.net
wikileaks.thomas-schwaab.de
wikileaks.hostmauher.com.ar
wikileaks.proyectoslum.com.ar
wiki.nlgshopping.nl
wl.temporalmenteinmortal.com
anl.to
wikileaks.teilin.net
wikileaks.rcrc.info
wikileaks.estsurinter.net
cableleaks.dyndns.org
wikileaks.worldtravelingartist.com
denardo.csclub.uwaterloo.ca
wikileaks.umleitung.com
wikileaks.alikati.com
wikileaks.bayofrum.net
www.wikileaks.belli-scientia.fr
wikileaks.moonwalker.fr
wikileaks.hostulo.us
www.wikilix.info
bruxelles-wikileaks.mooo.com
wikileaks.casafamelica.info ipv6
wikileaks.phoebo.net
wiki.leaksmirror.org
wikileaks.moonsorganics.nl
wikileaks.int80.de ipv6
wikileaks.manurevah.com
wikileaks.liioiil.com
wikileaks.douze-bis.net
wikilek.net
wikileaks.theoriginals.in
wikileaks.dlserv.de

wikileaks.siebinga.org
wikileaks.rubeninfante.com
scurvydawg.com
wikileaks.bisente.com
wikileaks.hiendlmayer.com.br
wikileaks.jhor.de
wikileaks.serveirc.com
wikileaks.idurar.com
wikileaks.jsfiles.de
wikileaks.reknet.ca
wikileaks.brokenarrow.me
wikileaks.johnb.uk.to
wikileaks.danielnoethen.de
transparency.net.ly
wikileaks.angidon.com
wiki.citizen-cam.de
www.wikileaksnostop.org
wikileaks.funderburg.me
wikileaks.centershock.net
wikileaks.liesdiemanpage.de
wikileaks.motociclism.md
wikileaks.marklamont.co.uk
wikileaks.voxlibre.info
wikileaks.cloppy.net
wikileaks.mun.io
wikileaks.davsebamse.dk
wikileaks.moonlit.no
wikileaks.filhodaputa.net
wikileaks.livex3m.cl
wl.luzi82.com
wikileaks.dirtyroadtrip.de
wikileaks2.bluug.org
wikileaks.gline.eu
wikileaks.vlshow.com
wikileaks.hayatimrap.com
wikileaks.fruitbattv.com
wikileaks.niasof.org
wikileaks.tedpennings.com
wikileaks.art-hacker.com
wikileaks.mutins.net
wikileaks.storns.net
wikileaks.network-pro.de
wikileaks.on.ht
wikileaks.gildamaurice.com
wikileaks.aswik.com
wikileaks.torkell.org
wikileaks.h-wd.ch
wikileaks.giest.info
leaks.phocks.org
wikileaks.gfxfreaks.com
wikileaks.malled.de ipv6
wikileaks.rbdspain.es
wikileaks.pbastida.net
wikileaks.actipc.fr
www.wikileaks.details-journal.fr
wikileaks.oslb.net
www.wikimee.info
www.wizards1strule.com
webitso.com
help.topwikileaks.cz.cc
wikileaks.net.ly
wikileaks.teralink.ca
wikileaks.alikati.com
wikileaks.nibbel.com
wikileaks.net.ly
wikileaks.preynokornews.info
www.wikileaks.hackersvault.com
wikileaks.zocuz.x10.mx
helpwikileaks.co.za
wikileaks.open-web.fr
wikileaks.ozazar.org
wikileaks.devhead.de
wikileaks.ishtar.ca
wikileaks.pitoo.com
wikileaks.libre-parcours.net ipv6
wikileaks.wehmut.de
wikileaks.sigkill.dk
wikileaks.corzani.no
wl.myrl.net
wikileaks.mysteryuniversity.com
wikileaks.wahrheitssuche.ch ipv6
wikileaks.kenin.fr
leaks.evilempire.no
wikileaks.m31.de
wikileaks.ephe.info
wikileaks.jeroenvanzijp.com
74.63.242.33
wikileaks.mysteryuniversity.com
wl.readafter.com
runatt.com
wikileaks.opennetguru.com
wikileaks.wind.at
wikileaks.fruitbattv.com
wikileaks.imdctech.ze.cx
wikileaks-nl.dyndns.org
wikileaks.fruitbattv.com
wikileaks.winkl11.de
wikileaks.q-soft.ch
freedom.reductioadabsurdum.org
wikileaks.marcwenger.ca
wikileaks.atanasov.eu
wikileaks.galiciaconfidencial.com
wikileaks.roath.eu
domaindelalutte.dyndns.org
wikileaks.x0.lv
mikeg26843.co.uk
wikileaks.zeira.org
wikileaks.wasweissich.net
wikileaks.boganking.com
wlcolombia.info
wikileaks.kirashi.ca
wikileaks.evos.com.au
www.wikileaks.nutfile.com ipv6
transparency.ly
wikileaks.org.ly
wikileaks.rezko.net
wikileaks.dohzya.com
wikileaks.adoshuv.net
wikileaks.nogui.net
wikileaks.libre.org
wl.cgan.de
wikileaks.firelab.net
wikileaks.alra7ba.info
wikileaks.pwnsauce.net
wikileaks.diinnz.com
wikileaks.openanthropology.org
wikileaks.blastermaster.nl
wikileaks.luxus-it.nl
wikileaks.rubrikk.no
94.247.169.134
wikileaks.liesdiemanpage.de
wl.worldtravelingartist.com
wl.genericdisclaimer.com
wikileaks.neeonline.com.br
wikileaks.amis.tv
wikileaks.tracciabi.li
wikileaks.livex3m.cl
wl.puck.fr ipv6
wikileaks.bnode.eu
www.gedankenverbrecher.org
wl.smeagol.de
wikileaks.n8sun.org
wikileaks.jackfolla.org
217.11.52.74:81
www.wikileaks.7u.cz ipv6
leaked.me
wlmr.dyndns.org
wikileaks.oldenleaks.de
wikileaks.cerebralcollective.com
canadapezkiwi.com.ar
66.197.179.65

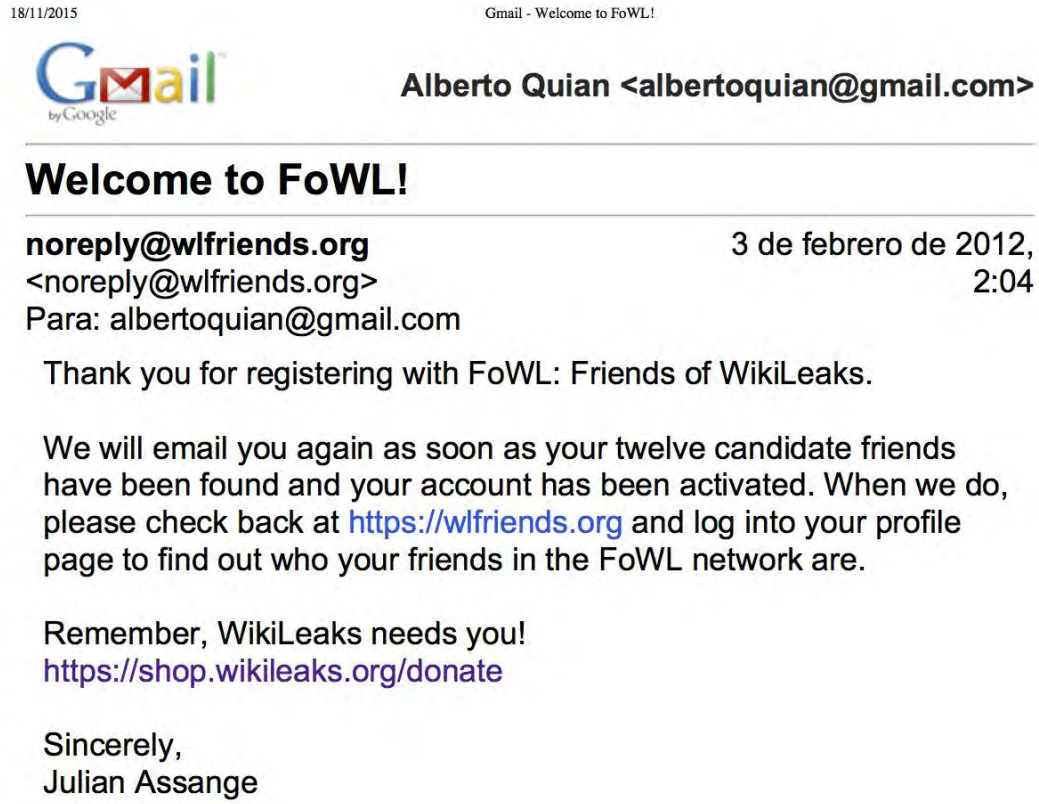
Fuente: Information Clearing House http://www.informationclearinghouse.info/article27007.htm

ANEXO II: Infografía del *Cablegate*. Distribución de los cables por países y años, y su clasificación.



Fuente: Pulse2 http://pulse2.com/2010/11/29/the-where-when-and-how-of-the-wikileaks-cables-infographic.

ANEXO III: Registro y participación en la red social WLFriends.



18/11/2015 Gmail - Welcome to FoWL!

Gmail by Google

Alberto Quian <albertoquian@gmail.com>

Welcome to FoWL!

noreply@wlfriends.org 3 de febrero de 2012, 2:04
<noreply@wlfriends.org>
Para: albertoquian@gmail.com

Thank you for registering with FoWL: Friends of WikiLeaks.

We will email you again as soon as your twelve candidate friends have been found and your account has been activated. When we do, please check back at https://wlfriends.org and log into your profile page to find out who your friends in the FoWL network are.

Remember, WikiLeaks needs you!
https://shop.wikileaks.org/donate

Sincerely,
Julian Assange

[FoWL] Important notice

Mail Manager <noreply@wlfriends.org>
Para: albertoquian@gmail.com

Dear FoWL member,

The FoWL network is ready to launch, and we have made substantial security upgrades. To become part of the network you must log in at

https://wlfriends.org/accounts/login

so that we can encrypt your account. This also gives you an opportunity to update your location and contact details. For the security of yourself and others we can't assign you friends until after you log in.

Some of you have already logged in, and so your account is already encrypted. However, a recent security upgrade means that all users MUST log in again; doing so automatically triggers an encrypted request to be assigned friends.

When you first log in, you will be given a secure login key. This one key is all that you will use for future logins; it replaces the username-password system. Your account will be completely unreadable without this key.

WARNING: Your secure login key cannot be reset. If you lose it, your entire account will be lost, without any possibility of recover!

Log in now to be part of the core network formation. WikiLeaks needs you.

-The WikiLeaks team.

##

Please log in to FoWL now!

Por favor, inicie sesión en FoWL ahora!

S'il vous plaît connectez-vous à FoWL maintenant!

Bitte loggen Sie sich jetzt in FoWL ein!

Effettua il login per FoWL ora!

Faça login para FoWL agora!

##

--
If you do not want to receive any more newsletters from us, log into your FoWL account and disable your email address in the profile settings.

--
powered by phpList, www.phplist.com --

Gmail

The first Friends of WikiLeaks friend assignment has been done!

Mail Manager <noreply@wlfriends.org>
Para: albertoquian@gmail.com

Dear albertoquian@gmail.com.

This is an important announcement about Friends of WikiLeaks.

The Friends of WikiLeaks network has been launched, and if you logged in at any point after June 2nd 2012 then you have been included in this first friendship network assignment. Please log in again at

https://wlfriends.org/accounts/login

to find out who your new friends are. For security reasons, your friends will only be able to see your details after you've logged in again, and you will be able to see theirs after they log in again.

If you haven't logged in since then, take this chance to do it now. This ensures that you will be included in the next network assignment.

Log in now to connect with other supporters. Check out your contacts, meet with them if practical, and if you think they're courageous, talented, diligent and committed, then start working with them to help WikiLeaks. If you find some of them unsuitable, you can drop them and we will find you new friends to replace them. It's up to you to keep your network as strong as possible!

Please log in to Friends of WikiLeaks now!

Por favor, inicie sesión en Friends of WikiLeaks ahora!

S'il vous plaît connectez-vous à Friends of WikiLeaks maintenant!

Bitte logge dich jetzt bei Friends of WikiLeaks ein!

Effettua il login per Friends of WikiLeaks ora!

Faça login para Friends of WikiLeaks agora!

--
If you do not want to receive any more newsletters from us, log into your FoWL account and disable your email address in the profile settings.

--
powered by phpList, www.phplist.com --

Gmail

Friends of WikiLeaks information email

Mail Manager <noreply@wlfriends.org>
Para: albertoquian@gmail.com

Dear albertoquian@gmail.com,

This is the first in a series of regular emails to members of Friends of WikiLeaks, designed to keep you informed about relevant WikiLeaks news and updates on the Friends of WikiLeaks community. These emails contain important information designed to help you participate as an active member and support WikiLeaks.

1. Friends of WikiLeaks latest friendship assignment round.

The latest friendship assignment round for Friends of WikiLeaks occurred on August 16th. We urge you to log in and find out about your new contacts. If you have made any drops since the previous round, then they will have been replaced. If you are new to the network and joined before the 16th, then you will have been given a full set of 12 new contacts. Remember, you won't be able to see your contacts until they have logged in, so please keep checking back at https://wlfriends.org/accounts/login . Why not take this opportunity to log in yourself now, so your new friends can see you!

2. Donating to WikiLeaks.

After being subjected to a relentless banking blockade for 18 months, WikiLeaks has found a way to accept credit card donations again. You can now donate by Visa or MasterCard, as well as many other methods, by visiting http://shop.wikileaks.org/donate#dccard. If you wish to donate by credit card, then please do so soon, as this method might not be available for very long. Without your support, WikiLeaks cannot continue to operate!

3. Problems with logging in to wlfriends.org .

Due to the popularity of Friends of WikiLeaks, it can sometimes take very long to log in, especially after a friendship assignment round. If log in is taking exceptionally long for you, then please be patient and do not navigate away from the login page. We have had reports of login taking up to 10 minutes, though this is rare.

4. Secure login key.

All new users of wlfriends.org have been given a secure login key to log in with. This replaces the old system of email + password. If you registered before May 31 2012, then we urge you to log in again at https://wlfriends.org/accounts/login. By doing so, your account will be fully encrypted, and you will be issued with a secure login key. It is important to keep this somewhere safe, as it is impossible for us to reset it.

5. Account problems in wlfriends.org .

The launch of the first friendship assignment round for Friends of WikiLeaks occured on July 2, 2012. This was an important milestone for us, as it transformed wlfriends.org from an idea into a proof of concept. We are happy to announce that the site is functioning well, but still not without some small problems.

A small number of users have informed us that they cannot log in with their secure login key. Unfortunately, some keys are not being issued correctly, and do not give access to the user's account. This problem is irreversible, and we cannot recover these accounts as we have no way of decrypting them. We urge you to log in as soon as you receive your secure login key. If you receive an error message that the key is invalid, then you will need to re-register. We apologise for any inconvenience this may cause, and hope to have it fixed soon.

We have recently received feedback from a small number users who are unable to edit their account details. We are now aware of this problem, and are working to fix it. If this problem affects you, then we ask that you be patient while we sort it out. Alternatively, you can register a new account which hopefully will not have the same problem.

6. WikiLeaks news resources.

The WikiLeaks twitter feed https://twitter.com/wikileaks is the main outlet for real-time updates about WikiLeaks and any important developments, run by WikiLeaks staff.

The blog http://www.thisdayinwikileaks.org/ is a great source of more broad and detailed news about WikiLeaks. It includes links to WikiLeaks releases, facts about the legal and political persecution of WikiLeaks staff and alleged sources, and information about upcoming events relating to WikiLeaks.

Gmail by Google

Friends of WikiLeaks information email

Mail Manager <noreply@wlfriends.org>
Para: albertoquian@gmail.com

Dear albertoquian@gmail.com,

This is an email to all members of Friends of WikiLeaks, designed to keep you informed about relevant WikiLeaks news and updates on the Friends of WikiLeaks community. These emails contain important information designed to help you participate as an active member and support WikiLeaks.

1. Secure connection to wlfriends.org

For the past two months the Friends of WikiLeaks website https://wlfriends.org was using a community-based certificate authority CAcert (www.cacert.org) . Many common operating systems did not recognise CAcert-issued certificates. This was not a problem with the security of wlfriends.org , but it did give many users an error message when they went to https://wlfriends.org . We have now reverted to a standard certificate authority, which is recognised by all standard operating systems. The SHA1 fingerprint of the new certificate is 5C:B1:0C:BB:D2:73:66:29:A8:F7:82:53:42:68:ED:4C:CF:BD:3F:DE For those who are interested, this can be verified by clicking the padlock next to the url in your browser.

2. Next Friends of WikiLeaks friendship assignment round

The Friends of WikiLeaks network is about to undergo its next friendship assignment round. This will consist of integrating newly registered member together with existing members who have dropped some of their contacts. If by now some of your assigned contacts still appear encrypted in your account then we suggest dropping them. This is very simple to do:

1. Log in to your account.

2. Click on their friend ID to go to their profile page.

3. Click on the red button at the bottom left of their profile 'Drop this contact and get another'.

4. Choose the most appropriate reason for dropping them. If they have not logged in yet then this would be 'This person never logged in, ...'.

For each contact you drop, you will be assigned another friend in the coming round. This will help you keep your network as strong as possible. The assignment will happen very soon, so please log in at https://wlfriends.org/accounts/login now to make sure you don't miss out!

3. Donating to WikiLeaks

After being subjected to a relentless banking blockade for almost two years, WikiLeaks has found a way to accept credit card donations again. You can now donate by Visa or MasterCard, as well as many other methods, by visiting http://shop.wikileaks.org/donate#dccard . If you wish to donate by credit card, then please do so soon, as this method might not be available for very long. Without your support, WikiLeaks cannot continue to operate!

As well as donating, you can support WikiLeaks by visiting https://beattheblockade.org/ and buying some WikiLeaks merchandise. There are lots of things to choose from, and they make excellent Christmas gifts. Every purchase made will help WikiLeaks continue to operate.

4. WikiLeaks news resources

The WikiLeaks twitter feed https://twitter.com/wikileaks is the main outlet for real-time updates about WikiLeaks and any important developments, run by WikiLeaks staff. The blog http://www.thisdayinwikileaks.org/ is a great source of more broad and detailed news about WikiLeaks. It includes links to WikiLeaks releases, facts about the legal and political persecution of WikiLeaks staff and alleged sources, and information about upcoming events relating to WikiLeaks.

5. Important article by Glenn Greenwald

Glenn Greenwald has been a vocal supporter of WikiLeaks for several years. He has recently written an article on the extra-judicial attacks on WikiLeaks and heavy handed legal proceedings on their supporters over the past 2 years. We believe that this article is so important for WikiLeaks supporters to read that we are including it, in full, at the end of this email. Everyone should find the time to read this article, as it gives a clear summary of the attacks on free speech that WikiLeaks and their supporters have had to endure.

Title: Prosecution of Anonymous activists highlights war for Internet control, by Glenn Greenwald.

http://www.guardian.co.uk/commentisfree/2012/nov/23/anonymous-trial-wikileaks-internet-freedom

---

Whatever one thinks of WikiLeaks, it is an indisputable fact that the group has never been charged by any government with any crime, let alone convicted of one. Despite that crucial fact, WikiLeaks has been crippled by a staggering array of extra-judicial punishment imposed either directly by the US and allied governments or with their clear acquiescence.

In December 2010, after WikiLeaks began publishing US diplomatic cables, it was hit with cyber-attacks so massive that the group was "forced to change its web address after the company providing its domain name cut off service". After public demands and private pressure from US Senate Homeland Security Chairman Joe Lieberman, Amazon then cut off all hosting services to WikiLeaks. Sophisticated cyber-attacks shortly thereafter forced the group entirely off all US website services when its California-based internet hosting provider, Everydns, terminated service, "saying it did so to prevent its other 500,000 customers of being affected by the intense cyber-attacks targeted at WikiLeaks".

Meanwhile, Chairman Lieberman's public pressure, by design, also led to the destruction of WikiLeaks' ability to collect funds from supporters. Master Card and Visa both announced they would refuse to process payments to the group, as did America's largest financial institution, Bank of America. Paypal not only did the same but froze all funds already in WikiLeaks' accounts (almost two years later, a court in Iceland ruled that a Visa payment processor violated contract law by cutting of those services). On several occasions in both 2011 and 2012, WikiLeaks was prevented from remaining online by cyber-attacks.

Over the past two years, then, this group - convicted of no crime but engaged in pathbreaking journalism that produced more scoops than all

other media outlets combined and received numerous journalism awards - has been effectively prevented from functioning, receiving funds, or even maintaining a presence on US internet servers. While it's unproven what direct role the US government played in these actions, it is unquestionably clear that a top US Senator successfully pressured private corporations to cut off its finances, and more important, neither the US nor its allies have taken any steps to discover and apprehend the perpetrators of the cyber-attacks that repeatedly targeted WikiLeaks, nor did it even investigate those attacks.

The ominous implications of all this have been never been fully appreciated. Recall that all the way back in 2008, the Pentagon prepared a secret report (ultimately leaked to WikiLeaks) that decreed WikiLeaks to be a "threat to the US Army" and an enemy of the US. That report plotted tactics that "would damage and potentially destroy" its ability to function. That is exactly what came to pass.

So this was a case where the US government - through affirmative steps and/or approving acquiescence to criminal, sophisticated cyber-attacks - all but destroyed the ability of an adversarial group, convicted of no crime, to function on the internet. Who would possibly consider that power anything other than extremely disturbing? What possible political value can the internet serve, or journalism generally, if the US government, outside the confines of law, is empowered - as it did here - to cripple the operating abilities of any group which meaningfully challenges its policies and exposes its wrongdoing?

But what makes all of this even more significant is the vastly disparate treatment of those who launched far less sophisticated and damaging attacks at those corporations which complied with US demands and cut off all funding and other services to WikiLeaks. Acting in the name of Anonymous, a handful of activists targeted those companies with simple "denial of service" attacks, ones that impeded the operations of those corporate websites for a few hours.

In stark contrast to the far more significant attacks aimed at WikiLeaks, these attacks, designed to protest the treatment of WikiLeaks, spawned a global manhunt by western nations and, ultimately, the arrest of dozens of mostly young alleged hackers, four of whom are now on trial in London:

"Four activists from the hackers collective Anonymous caused multimillion-pound losses to a number of firms in revenge for the backlash against WikiLeaks, a court has heard.

"Using the name Operation Payback, the four flooded websites belonging to companies including PayPal and Ministry of Sound with messages and requests in order to bring them down. . . .The self-styled 'hactivists' caused losses worth more than $3.5m at PayPal and caused sites belonging to MasterCard and the recording industry to go offline.

"Three of the group have admitted their role in the conspiracy. Christopher Weatherhead, 22, a student at Northampton University, is on trial at Southwark crown court accused of being 'part of a small cabal of leaders' of the cyber-attacks...

"The four used a free internet tool called Low Orbit Ion Canon (LOIC) as a 'destructive cyber weapon', the court heard. 'Once downloaded, the LOIC could be used to attack by sending internet traffic to a target computer,' said. 'When the volume of traffic sent to a computer becomes too much for it to handle it would suffer a denial of service. The more LOICs used, therefore, to attack a target computer, the more likely that a denial of service will take place.'"

Last year, the FBI arrested 16 people in the US in connection with similar attacks on Master Card, Visa and Amazon, and charged them with crimes that carry 10-year prison terms.

The issue here is not whether Anonymous activists can be rightfully prosecuted: acts of civil disobedience, by definition, are violations of the law designed to protest or create a cost for injustices. The issue is how selectively these cyber-attack laws are enforced: massive cyber-attacks aimed at a group critical of US policy (WikiLeaks) were either perpetrated by the US government or retroactively sanctioned by it, while relatively trivial, largely symbolic attacks in defense of the group were punished with the harshest possible application of law enforcement resources and threats of criminal punishment.

That the US government largely succeeded in using extra-legal and extra-judicial means to cripple an adverse journalistic outlet is a truly consequential episode: nobody, regardless of one's views on WikiLeaks, should want any government to have that power. But the manifestly overzealous prosecutions of Anonymous activists, in stark contrast to the (at best) indifference to the attacks on WikiLeaks, makes all of that even worse. In line with its unprecedented persecution of whistleblowers generally, this is yet another case of the US government exploiting the force of law to entrench its own power and shield its actions from scrutiny.

Gmail

The next Friends of WikiLeaks friendship assignment has been done!

Mail Manager <noreply@wlfriends.org>
Para: albertoquian@gmail.com

Dear albertoquian@gmail.com.

This is an important announcement about Friends of WikiLeaks.

1. Friendship assignment

The next Friends of WikiLeaks friendship assignment has now been done. Please log in again at https://wlfriends.org/accounts/login to find out who your new friends are. For security reasons, your friends will only be able to see your details after you log in again, and you will be able to see theirs after they log in again.

Log in now to connect with other supporters. Check out your contacts, meet with them if practical, and if you think they're courageous, talented, diligent and committed, then start working with them to help WikiLeaks. If you find some of them unsuitable, or they have not logged in after a long time (over 2 weeks), you can drop them and we will find you new friends to replace them. It's up to you to keep your network as strong as possible!

2. Users receiving fewer than six global contacts

For the moment, some users may not be receiving a full set of six global contacts. We are aware of this problem, and are doing our best to rectify it. Automating the friendship assignment of many thousands of supporters has been a difficult task, and we hope to have it working properly soon. The assignment of local contacts is unaffected by this problem.

3. Login time

Due to the highly secure encryption schemes used on wlfriends.org, loggin in to your account might take up to 30 seconds. We apologise for this, and hope that you understand the necessity for it.

4. Donations to WikiLeaks

There are now several ways to donate to Wikileaks. These are all listed at http://shop.wikileaks.org/donate . You can also donate to Wikileaks, and many other worthy news organisations, via the Freedom of the Press Foundation https://pressfreedomfoundation.org/ . Without your support, WikiLeaks cannot continue to operate!

Please log in to Friends of WikiLeaks now!

Por favor, inicie sesión en Friends of WikiLeaks ahora!

S'il vous plaît connectez-vous à Friends of WikiLeaks maintenant!

Bitte logge dich jetzt bei Friends of WikiLeaks ein!

Effettua il login per Friends of WikiLeaks ora!

Faça login para Friends of WikiLeaks agora!

ANEXO IV: Invitación exclusiva para investigar los *Syria Files*.

Gmail by Google

Alberto Quian <albertoquian@gmail.com>

Exclusive WikiLeaks Invite for the Syria Files

signup@wikileaks.org 12 de septiembre de 2012, 21:11
<signup@wikileaks.org>
Para: albertoquian@gmail.com

You have been confidentially invited to join the WikiLeaks investigative group for the Syria Files – more than two million emails from Syrian political figures, ministries and associated companies, dating from August 2006 to March 2012. This extraordinary data set derives from 680 Syria-related entities or domain names, including those of the Ministries of Presidential Affairs, Foreign Affairs, Finance, Information, Transport and Culture. The Syria Files shine a light on the inner workings of the Syrian government and economy, but they also reveal how the West and Western companies say one thing and do another. The range of information extends from the intimate correspondence of the most senior Baath party figures to records of financial transfers sent from Syrian ministries to other nations. Being part of this international team will put you in the privileged position of being able to search the emails using the sophisticated WikiLeaks search engine which will enable you to research and publish articles and papers using this data.

We have created a unique invitation system that allows selected journalists, University Professors and employees of human rights organisations to join this project. The system allows the selected invitees, such as yourself, to agree to our Terms and Conditions and gain immediate access to the files for research and publishing purposes, and to invite others worthy of inclusion.

To join this project go to the following URL:

http://wikileaks.org/SyriaFiles-Signup-Instructions.html

Here you will be given full instructions on the simple steps to join this project. Follow the instructions to reach the Terms and Conditions page where you will be asked to enter your invite code. Your unique invite code is:

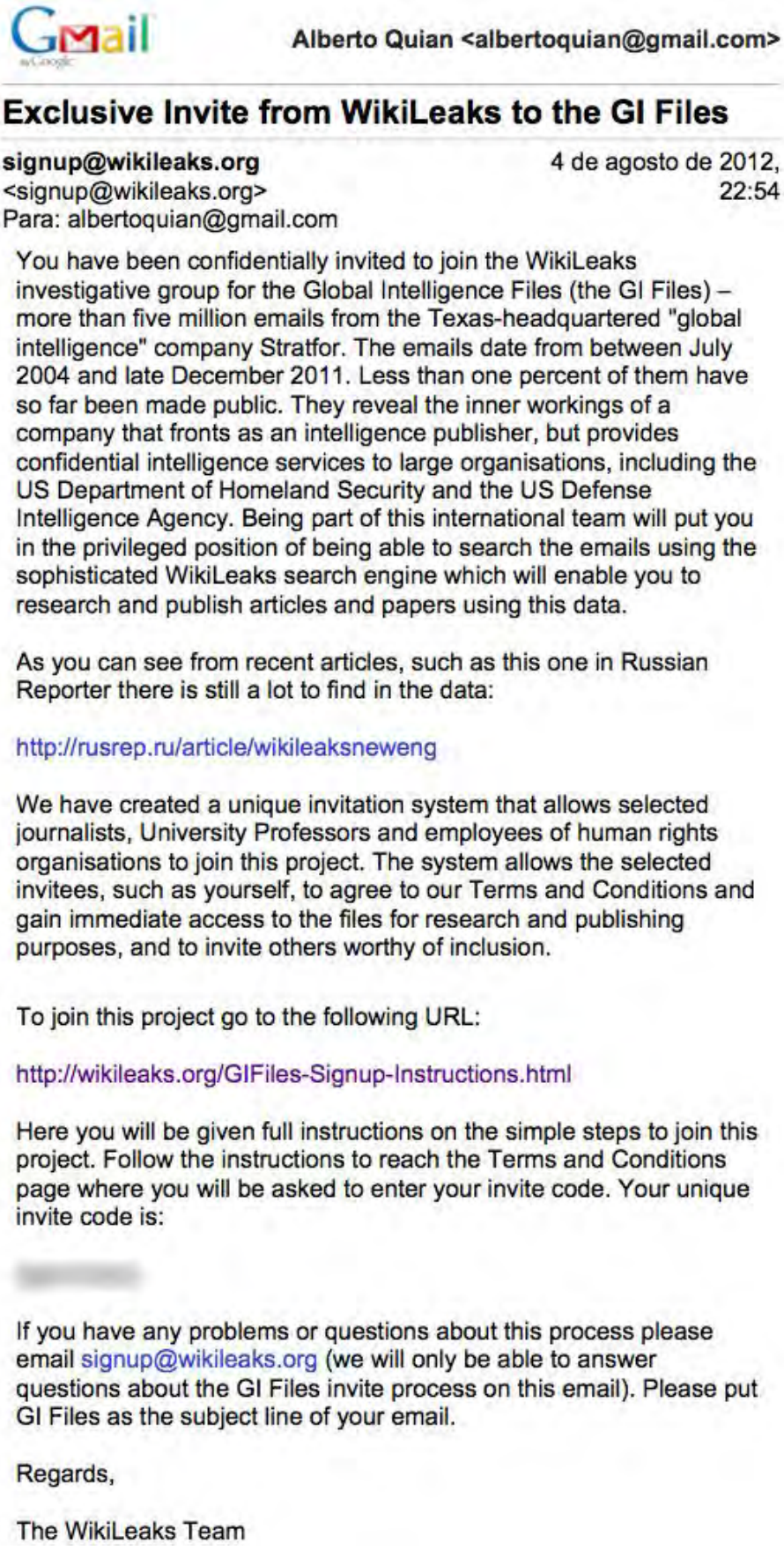
[redacted]

If you have any problems or questions about this process please email signup@wikileaks.org (we will only be able to answer questions about the Syria Files invite process on this email). Please put Syria Files as the subject line of your email.

Regards,

The WikiLeaks Team

ANEXO V: Invitación exclusiva para investigar los *GI Files*.



Alberto Quian <albertoquian@gmail.com>

Exclusive Invite from WikiLeaks to the GI Files

signup@wikileaks.org 4 de agosto de 2012, 22:54
<signup@wikileaks.org>
Para: albertoquian@gmail.com

You have been confidentially invited to join the WikiLeaks investigative group for the Global Intelligence Files (the GI Files) – more than five million emails from the Texas-headquartered "global intelligence" company Stratfor. The emails date from between July 2004 and late December 2011. Less than one percent of them have so far been made public. They reveal the inner workings of a company that fronts as an intelligence publisher, but provides confidential intelligence services to large organisations, including the US Department of Homeland Security and the US Defense Intelligence Agency. Being part of this international team will put you in the privileged position of being able to search the emails using the sophisticated WikiLeaks search engine which will enable you to research and publish articles and papers using this data.

As you can see from recent articles, such as this one in Russian Reporter there is still a lot to find in the data:

http://rusrep.ru/article/wikileaksneweng

We have created a unique invitation system that allows selected journalists, University Professors and employees of human rights organisations to join this project. The system allows the selected invitees, such as yourself, to agree to our Terms and Conditions and gain immediate access to the files for research and publishing purposes, and to invite others worthy of inclusion.

To join this project go to the following URL:

http://wikileaks.org/GIFiles-Signup-Instructions.html

Here you will be given full instructions on the simple steps to join this project. Follow the instructions to reach the Terms and Conditions page where you will be asked to enter your invite code. Your unique invite code is:

If you have any problems or questions about this process please email signup@wikileaks.org (we will only be able to answer questions about the GI Files invite process on this email). Please put GI Files as the subject line of your email.

Regards,

The WikiLeaks Team

ANEXO VI: Instrucciones de registro para los *GI Files*.

GIFiles Signup Instructions

Becoming a WikiLeaks Partner for the Global Intelligence Files

You have been invited to enter a secret world.

By joining the global WikiLeaks partnership on the Global Intelligence Files (the GI Files) – you will have access to more than five million emails from the Texas-headquartered "global intelligence" company Stratfor. The emails date from between July 2004 and late December 2011. They reveal the inner workings of a company that fronts as an intelligence publisher, but provides confidential intelligence services to large organisations, including the US Department of Homeland Security and the US Defense Intelligence Agency. Being part of this international team will allow you to search the emails using the sophisticated search engine designed by WikiLeaks to enable you to research and publish articles and papers using this data.

The purpose of this system is to maximise global impact of the GI Files by restricting supply to those who are most likely to research and publish on them.

We are allowing journalists, academics and human rights organisations to search and publish the GI Files. To enter into this partnership you will need to be given a unique code by one of our existing partners. Users who demonstrate research and publishing ability will be considered as partners for new WikiLeaks publications.

Once you have this code please follow the instructions below to enter the partnership and gain access to the GI Files. These instructions are designed to be idiot-proof. They explain every step of this process, but don't be scared - for most people this will be quick.

1. Download Tor, a tool for encrypted anonymous web-browsing. Without this you will not be able to access our Terms and Conditions, or the GI Files database.

Tor Instructions:
- To get Tor please go to the following URL to download the "Tor Browser Bundle:" https://www.torproject.org/projects...
- Choose the correct version depending on whether you use Windows, Mac or Linux and download it in the language you want.
- Click on the correct version to download it and then save it - we suggest to your Desktop.
- Once you have saved it you can find the "Tor Browser Bundle" application in the place you saved it.
- You will need to double-click on the Start Tor browser application to run Tor.
- You will need Tor running to access the site to agree to our Terms and Conditions, and then to later access the GI Files site.

2. Start Tor and go to the following site (it will only work using Tor). Wait up to 30 seconds for the site to load for the first time: http://7f4lihm464gdcwfc.onion/invite/step1

3. Enter your unique invite code to get access to the GI Files partner Terms and Conditions.

4. Enter your name, organisation name, email address and phone number. The email address you give cannot be a personal email address; it must be a work email account.

5. Read all parts of the Terms and Conditions and make sure you understand them. If you have any questions, please email: signup@wikileaks.org

6. Once you understand your responsibilities under the Terms and Conditions tick the check box to confirm your agreement.

7. Within 15 minutes you will receive an email to the email address you supplied giving you login details to the GI Files website.

8. Login to the site at the following URL: http://7f4lihm464gdcwfc.onion/ giving your username and password as supplied in the email. This URL can only be accessed when using Tor.

9. Once you are logged into the site you will see your user page, the search interface and publishing interface. At the top of the page are tabs that explain how these work. On your user page you will have five invite codes for you to give to others so that they can also gain access to the GI Files.

10. If you wish to invite someone to the GI Files then give them a unique invite code, along with the URL to this page of instructions - each person you invite must be a journalist, NGO worker or academic from a different organisation (for complete understanding of who you can invite please see the invite rules below). You will find 5 invite codes to give out on your 'My Account' page.

11. If you violate any of the Terms and Conditions you risk having your login terminated, along with that of the person that invited you and the people that you invited. If any of the contacts you invited violate the terms of the Terms and Conditions, they risk having their login terminated, your login terminated and the logins of the people they invited terminated.

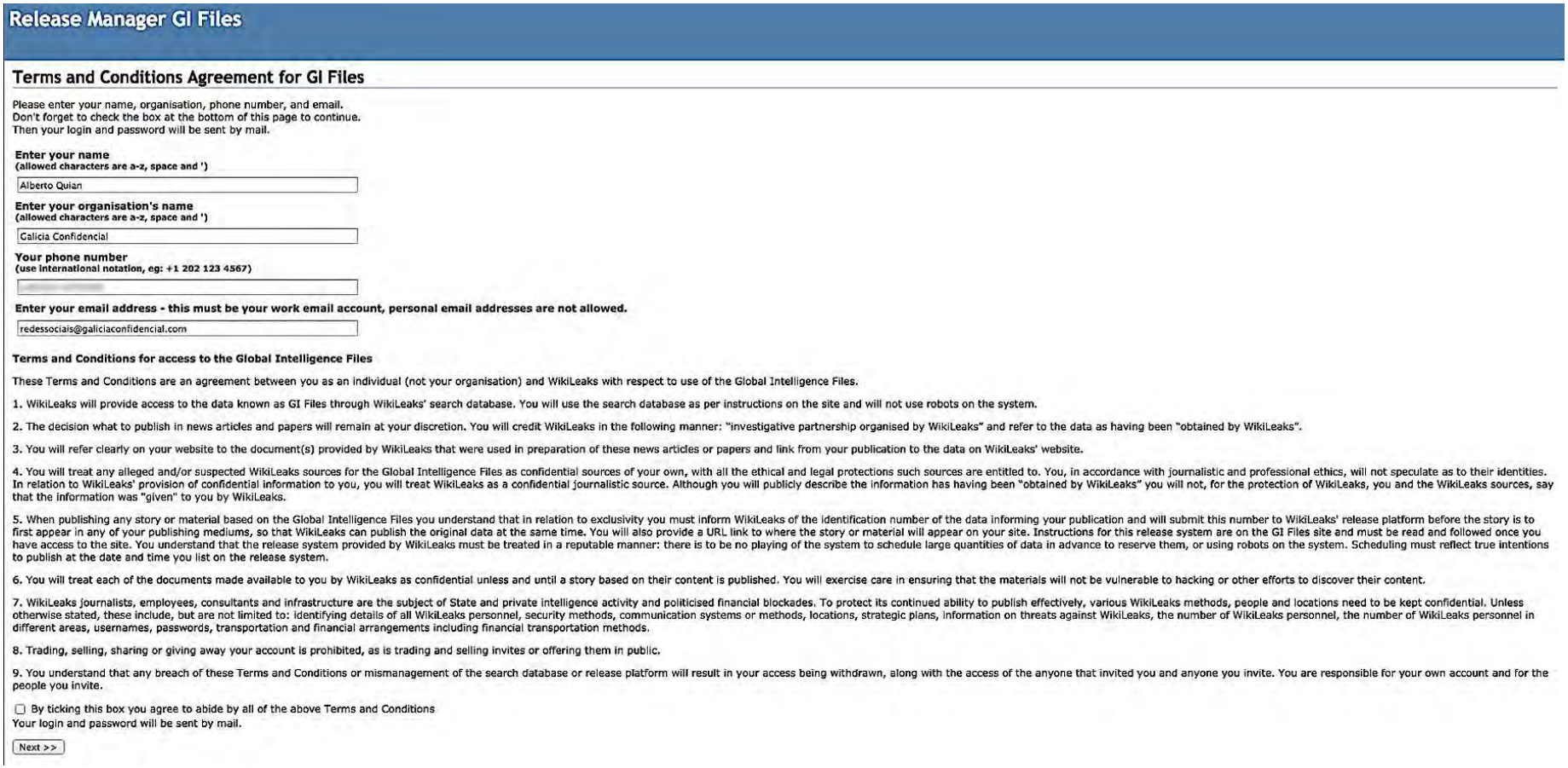
12. There are two chat channels that you can use for this process and discuss things related to this process with others:
    if you are having issues with tor please go to the following channel and speak to others about this: https://crypto.cat/?c=torissues
    once you are working on the database please go to the following channel (that can only be accessed through tor) and discuss your findings, issues and tips: http://brm5vfq7o4dtdqxz.onion/?chan...

Invite Rules:

Each invite code must be given to a person who:
A. is a real person
B. is either a journalist, Professor or Associate Professor at a University or an employee of a human rights organisation
C. is from a different organisation to you and your other invitees
D. is using an email that is not a personal email
E. is using an email that is from a different domain to your email address and that of the other people you invite
F. is going to use the GI Files search and release site for research, the results of which will be communicated to the public.

For any issues or questions related to this signup process, please email: signup@wikileaks.org

ANEXO VII: Condiciones de uso de los *GI Files*.



Release Manager GI Files

Terms and Conditions Agreement for GI Files

Please enter your name, organisation, phone number, and email.
Don't forget to check the box at the bottom of this page to continue.
Then your login and password will be sent by mail.

Enter your name
(allowed characters are a-z, space and ')

Alberto Quian

Enter your organisation's name
(allowed characters are a-z, space and ')

Galicia Confidencial

Your phone number
(use international notation, eg: +1 202 123 4567)

Enter your email address - this must be your work email account, personal email addresses are not allowed.

redessociais@galiciaconfidencial.com

Terms and Conditions for access to the Global Intelligence Files

These Terms and Conditions are an agreement between you as an individual (not your organisation) and WikiLeaks with respect to use of the Global Intelligence Files.

1. WikiLeaks will provide access to the data known as GI Files through WikiLeaks' search database. You will use the search database as per instructions on the site and will not use robots on the system.

2. The decision what to publish in news articles and papers will remain at your discretion. You will credit WikiLeaks in the following manner: "investigative partnership organised by WikiLeaks" and refer to the data as having been "obtained by WikiLeaks".

3. You will refer clearly on your website to the document(s) provided by WikiLeaks that were used in preparation of these news articles or papers and link from your publication to the data on WikiLeaks' website.

4. You will treat any alleged and/or suspected WikiLeaks sources for the Global Intelligence Files as confidential sources of your own, with all the ethical and legal protections such sources are entitled to. You, in accordance with journalistic and professional ethics, will not speculate as to their identities. In relation to WikiLeaks' provision of confidential information to you, you will treat WikiLeaks as a confidential journalistic source. Although you will publicly describe the information has having been "obtained by WikiLeaks" you will not, for the protection of WikiLeaks, you and the WikiLeaks sources, say that the information was "given" to you by WikiLeaks.

5. When publishing any story or material based on the Global Intelligence Files you understand that in relation to exclusivity you must inform WikiLeaks of the identification number of the data informing your publication and will submit this number to WikiLeaks' release platform before the story is to first appear in any of your publishing mediums, so that WikiLeaks can publish the original data at the same time. You will also provide a URL link to where the story or material will appear on your site. Instructions for this release system are on the GI Files site and must be read and followed once you have access to the site. You understand that the release system provided by WikiLeaks must be treated in a reputable manner: there is to be no playing of the system to schedule large quantities of data in advance to reserve them, or using robots on the system. Scheduling must reflect true intentions to publish at the date and time you list on the release system.

6. You will treat each of the documents made available to you by WikiLeaks as confidential unless and until a story based on their content is published. You will exercise care in ensuring that the materials will not be vulnerable to hacking or other efforts to discover their content.

7. WikiLeaks journalists, employees, consultants and infrastructure are the subject of State and private intelligence activity and politicised financial blockades. To protect its continued ability to publish effectively, various WikiLeaks methods, people and locations need to be kept confidential. Unless otherwise stated, these include, but are not limited to: identifying details of all WikiLeaks personnel, security methods, communication systems or methods, locations, strategic plans, information on threats against WikiLeaks, the number of WikiLeaks personnel, the number of WikiLeaks personnel in different areas, usernames, passwords, transportation and financial arrangements including financial transportation methods.

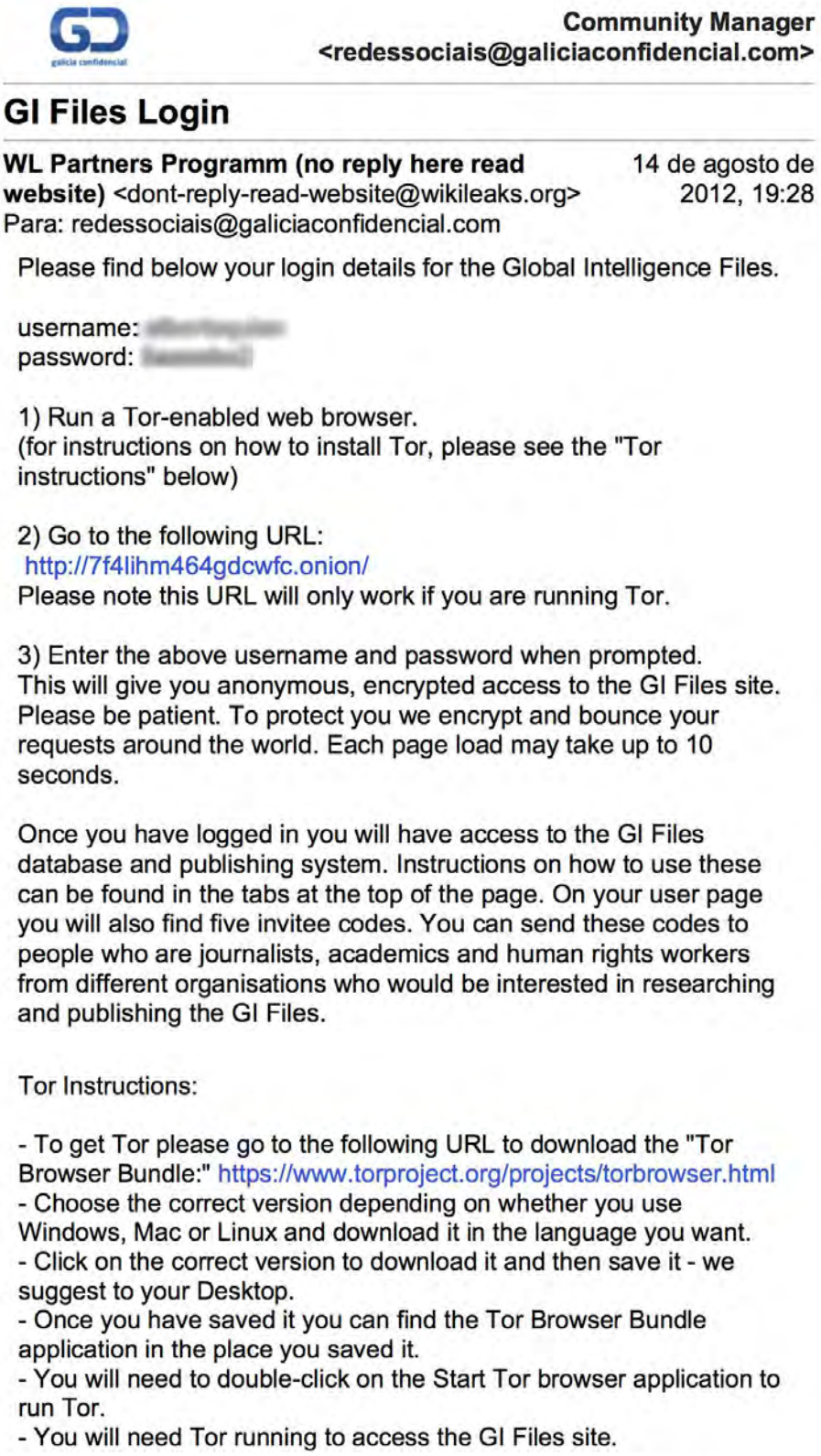
8. Trading, selling, sharing or giving away your account is prohibited, as is trading and selling invites or offering them in public.

9. You understand that any breach of these Terms and Conditions or mismanagement of the search database or release platform will result in your access being withdrawn, along with the access of the anyone that invited you and anyone you invite. You are responsible for your own account and for the people you invite.

☐ By ticking this box you agree to abide by all of the above Terms and Conditions
Your login and password will be sent by mail.

Next >>

ANEXO VIII: Correo de confirmación de registro en los *GI Files*.



Community Manager
<redessociais@galiciaconfidencial.com>

GI Files Login

WL Partners Programm (no reply here read website) <dont-reply-read-website@wikileaks.org> 14 de agosto de 2012, 19:28
Para: redessociais@galiciaconfidencial.com

Please find below your login details for the Global Intelligence Files.

username: [redacted]
password: [redacted]

1) Run a Tor-enabled web browser.
(for instructions on how to install Tor, please see the "Tor instructions" below)

2) Go to the following URL:
http://7f4lihm464gdcwfc.onion/
Please note this URL will only work if you are running Tor.

3) Enter the above username and password when prompted.
This will give you anonymous, encrypted access to the GI Files site.
Please be patient. To protect you we encrypt and bounce your requests around the world. Each page load may take up to 10 seconds.

Once you have logged in you will have access to the GI Files database and publishing system. Instructions on how to use these can be found in the tabs at the top of the page. On your user page you will also find five invitee codes. You can send these codes to people who are journalists, academics and human rights workers from different organisations who would be interested in researching and publishing the GI Files.

Tor Instructions:

- To get Tor please go to the following URL to download the "Tor Browser Bundle:" https://www.torproject.org/projects/torbrowser.html
- Choose the correct version depending on whether you use Windows, Mac or Linux and download it in the language you want.
- Click on the correct version to download it and then save it - we suggest to your Desktop.
- Once you have saved it you can find the Tor Browser Bundle application in the place you saved it.
- You will need to double-click on the Start Tor browser application to run Tor.
- You will need Tor running to access the GI Files site.

ANEXO IX: Publicación 1 de los correos de Stratfor.

A maior compañía de espionaxe do mundo vixía o independentismo galego

Stratfor Global Intelligence cualificou en 2010 como "leve" o movemento secesionista en Galicia e salientou que "dende 1990 o BNG foi abandonando o discurso separatista". GC accedeu, a través dun convite confidencial de WikiLeaks, aos máis de 5 millóns de correos electrónicos filtrados da que é coñecida como "a CIA na sombra". Correos electrónicos en PDF no interior.

› GC accede aos emails que WikiLeaks filtrou da axencia de intelixencia Stratfor

Por Alberto Quian | Madrid | 21/08/2012 | Actualizada ás 11:00

"O movemento polo secesionismo é moi leve en Galicia". Así o sentencia un breve informe da compañía de espionaxe privada Stratfor Global Intelligence. GC tivo acceso a este documento a través dun convite confidencial de WikiLeaks para consultar a enorme base de datos cos máis de 5 millóns de correos electrónicos que obtivo WikiLeaks desta empresa de intelixencia global, coñecida entre os analistas como "a CIA na sombra".

Stratfor é a maior compañía de intelixencia do mundo.

O devandito correo electrónico foi enviado o 28 de xullo de 2010 pola informante Elodie Dabbagh á sección de análise para Eurasia de Stratfor Global Intelligence. Neste correo electrónico, enviado co asunto "[Eurasia] TASKING - Secessionism", Dabbagh cualifica as principais correntes independentistas en Europa, iniciando o seu informe cunha sucinta análise da situación do nacionalismo galego.

"Procurarei ser breve, pero se pode ampliar se é necesario", comeza escribindo Dabbagh para logo dar conta da situación dos movementos secesionistas en Europa, incluídos os de Euskadi, Cataluña, a provincia autónoma de Nagorno Karabaj (Acerbaixán), Bélxica, Córcega (Francia) e o pobo saami en Noruega, Finlandia, Suecia e Rusia.

O breve informe foi remitido seis días despois de que o Tribunal Internacional de Xustiza da ONU sentenciase que a declaración secesionista de Kosovo do 17 de febreiro de 2008 non vulneraba o dereito internacional. Foi precisamente este feito o que motivou a comunicación entre a informante de Stratfor e a sección para asuntos en Eurasia para analizar o estado dalgúns movementos secesionistas e o seu parecer sobre a independencia de Kosovo.

Secesionismo galego

Elodie Dabbagh comeza a súa breve análise sobre o secesionismo en Eurasia abordando o caso do nacionalismo galego. Neste caso non existen referencias que vinculen dalgún xeito o independentismo kosovar e galego. Dabbagh céntrase en describir a composición do Parlamento de Galicia e a situación da corrente nacionalista a través de mínimas pinceladas.

Se hai algo que pasma ao ler o correo de Dabbagh é a cifra que dá sobre a poboación galega. Segundo a informante de Stratfor, existen "aproximadamente 10 millóns de galegos no mundo, inluíndo 2.796.089 en Galicia (6-7% da poboación de España)", sinala no seu informe. A informante non sinala ningunha fonte da que supostamente obtivo estes datos que ninguén coñece. De feito, os datos oficiais son notablemente menores: no ano 2010 había oficialmente 401.068 galegos residentes no estranxeiro, segundo datos do Instituto Galego de Estatística (IGE), aos que habería que sumar outros preto de 400.000 residentes noutras comunidades autónomas do Estado español. E os analistas máis atrevidos falan darredor de 1,3 millóns de emigrados, ampliando a identidade galega a varias xeracións.

A partir de aquí, a informante de Stratfor céntrase en describir o movemento nacionalista galego. Dabbagh salienta que "o apoio popular á independencia" é "baixo" en Galicia, e para xustificar esta conclusión fai referencia a "unha enquisa recente" da que non ofrece a fonte, na que se conclúe que "o 75% dos galegos se senten máis españois que galegos".

Dabbagh tamén sinala que Galicia "conta cun autogoberno parcial, na forma du goberno con transferencias, creado o 16 de marzo de 1978 e reforzado polo Estatuto de Autonomía de Galicia, ratificado o 28 de abril 1981".

Logo pasa a describir a composición actual do Parlamento de Galicia para dar paso a unha breve valoración da evolución do discurso do BNG nos últimos vinte anos:

"Dende 1990 o BNG foi abandonando o discurso secesionista e as reclamacións de autodeterminación rara vez se producen, sobre todo dende que o partido rexionalista Unidade Galega se uniu á coalición", explica Dabbagh.

Finalmente, Elodie Dabbagh conclúe que "o movemento polo secesionismo é moi leve en Galicia".

Lista de rexións secesionistas

Este correo electrónico enviado por Elodie Dabbagh responde a outra serie de *e-mails* intercambiados entre varios informantes de Stratfor e o vicepresidente de Intelixencia Estratéxica, Rodger Baker, para elaborar unha ampla lista coordinada polo analista xeopolítico Marko Papic cos movementos indepentistas máis importantes na rexión de Eurasia.

Neses correos vanse propoñendo listas de rexións por países agrupadas e clasificadas nunha escala de cinco niveis segundo a intensidade dos movementos secesionistas, sendo I a máis baixa e V a máis alta. Cada rexión asígnase a un informante.

Papic fala neses correos de poñer en marcha unha serie de "tarefas sobre o secesionismo en Europa" para "evaluar [...] a través das nosas fontes a situación das rexións secesionistas de Europa".

Papic sinala nun principio que o equipo terá que clasificar as distintas rexións en "catro niveis de secesionismo", mais finalmente, nun intercambio de correos co departamento de analistas de Stratfor e con George Friedman —o ideólogo e fundador desta compañía de intelixencia— envía a lista definitiva con cinco niveis de intensidade das correntes indepentistas xunto cos breves informes elaborados polos seus colaboradores.

Nivel I: o secesionismo é algo que se "coce a fogo lento", sinala Papic, quen engade: "Si, o secesionismo é unha idea, pero a rexión non ten ningún interese en perseguila", se ben "podería suceder nalgún momento no futuro se as condicións son as axeitadas ou cambian", comenta aos seus compañeiros. Neste grupo inclúe a Galicia, ademais de Lombardia (Italia), Krajina (Croacia), Vojvodina (Serbia), Tartaristán (Rusia) e as terras dos saami en Noruega, Finlandia e Suecia.

Nivel II: "O secesionismo está activo pero é débil", indica Papic, quen explica: "O secesionismo é máis que unha idea lonxana -cando non un obxectivo declarado abertamente-, é un desexo, pero a rexión non dispón de medios na procura da mesma; é moi débil". Neste grupo inclúen ao País Vasco, Herzegovina Occidental (Federación de Bosnia y Herzegovina), Carpato-Rutenia (Ucraína), Sandžak (Serbia e Montenegro), Crimea (Ucraína) e as terras dos székely en Romanía.

Nivel III: segundo Papic, o independentismo é "activo", pero "sen violencia". "O secesionismo é o obxectivo declarado, pero a rexión non usa a violencia para acadalo", comenta o analista. Neste grupo inclúe a Cataluña, Bélxica, Groenlandia (Dinamarca), Illas Feroe (Dinamarca) e Escocia.

Nivel IV: Papic fala de secesionismo "activo" con "posible violencia". Para o analista de Stratfor, "o secesionismo é o obxectivo declarado e a violencia, un medio potencial (ou activo) para acadala". Papic inclúe neste nivel a Republica Srpska (Bosnia), Transnistria (Moldavia), a rexión albanesa de Macedonia, Kosovo do Norte (Serbia), Nagorno Karabaj (Acerbaixán), Adjara e Samtskhe-Javaheti (Georgia) e as repúblicas da Federación Rusa de Chechenia, Ingusetia, Kabardia-Balkaria, Bashkortostán, Adygea, Karachai-Cherkessia e Osetia do Norte.

Nivel V: neste nivel Papic inclúe as rexións nas que "a secesión é un feito" pero "a violencia aínda é posible". Aquí inclúe a Osetia do Sur e Abxacia.

Metodoloxía

Marko Papic sinala no intercambio de correos que "metodoloxicamente se necesitan cinco cousas" para analizar as distintas rexións:

1. A resposta de cada rexión ao fallo da Corte Internacional de Xustiza sobre a declaración de independencia de Kosovo.
2. Unha evaluación do apoio exterior a cada rexión.
3. O apoio popular á secesión.
4. Unha evaluación da autoridade -política e/ou militar- do territorio.
5. Consultar a fontes na rexión como perciben a decisión da Corte Internacional de Xustiza e que vai ser o seguinte.

Medios de comunicación

No correo enviado a Rodger Baker, Marko Papic consideraba que os medios de comunicación están a errar ao concentrar a atención nas "rexións equivocadas". Papic adiantaba que a independencia de Kosovo e a opinión da Corte Internacional de Xustiza tería "un impacto menor nas rexións da antiga Unión Soviética" e consideraba que era en Europa Occidental e os Balcáns onde a decisión da Corte Internacional tería "un maior impacto".

"Nos Balcáns, debido á aplicabilidade directa para a República Srpska en Bosnia e Herzegovina, e para os albaneses en Macedonia; e en Europa Occidental, debido a que unha opinión da Corte Internacional de Xustiza e a lexitimidade xurídica teñen moito máis peso en España ou Reino Unido que en Acerbaixán e Rusia", xustifica Papic.

Descarga os correos electrónicos de Stratfor

http://www.galiciaconfidencial.com/ficheros/2012_8_20_13202.pdf.

http://www.galiciaconfidencial.com/ficheros/2012_8_20_13203.pdf

http://www.galiciaconfidencial.com/ficheros/2012_8_20_13205.pdf

Tamén se pode consultar a nova de GC dende a páxina web de WikiLeaks.

ANEXO X: Publicación 2 de los correos de Stratfor.

Un analista de Stratfor aconsellou facer un seguimento a Resistencia Galega

Segunda achega sobre os emails da compañía de intelixencia global aos que tivo acceso GC a través de WikiLeaks. Un informante de Stratfor advertiu en 2011 da crecente actividade de Resistencia Galega e a debilidade de ETA. Outro informe de Scotland Yard de 2007 informaba das accións do grupo armado galego. Descarga os documentos en GC Plus.

- A maior compañía de espionaxe do mundo vixía o independentismo galego
- GC accede aos emails que WikiLeaks filtrou da axencia de intelixencia Stratfor
- Emails de Stratfor e documento de Scotland Yard sobre Resistencia Galega

Por Alberto Quian | Madrid | 27/08/2012 | Actualizada ás 11:00

A crecente actividade de Resistencia Galega e a debilidade de ETA fixeron repensar aos analistas de Stratfor a cuestión da loita armada no Estado español no ano 2011. Un analista desta compañía de intelixencia global, sita en Texas, aconselleu facer un seguimento ao grupo separatista galego, ao que se lle atribuían supostos vínculos con ETA.

Ataque de Resistencia Galega contra as obras do AVE

O 18 de xaneiro de 2011, o analista táctico Ben West e a vicepresidenta de Marketing Internacional de Stratfor, Antonia Colibasanu, mantiveron un intercambio de correos electrónicos co departamento de Análises da compañía sobre as accións de Resistencia Galega nos que se advertía de ameazas terroristas a cargos políticos en Galicia. Así o sinalaban no propio asunto destes *emails*: "Blast targets political office in Spain's Galicia region".

West e Colibasanu enviaron unha recompilación de noticias sobre os últimos atentados do grupo armado galego. No seu *email*, Ben West comezaba a súa comunicación cunha sucinta explicación cos motivos polos que aconsellaba facerlle un seguimento a Resistencia Galega:

> "Máis detalles sobre estes tipos a continuación. Eles foron responsábeis de polo menos 13 ataques en 2010. Parecen moi pequenos, pero supostamente teñen vínculos con ETA. Sería interesante se estes tipos repuntan a medida que ETA mingua".

Neste correo electrónico, Ben West achegaba unha información en inglés publicada en Ansa Mediterranean (ANSAmed), —sección da Agenzia Nazionale Stampa Associata— sobre as accións de Resistencia Galega, sobre a que xustificaba a súa recomendación de seguir os pasos do grupo separatista galego. Co título "Spain: Galician separitists new terrorism front" ("España: nova fronte terrorista de separatistas galegos"), a axencia italiana informaba o 20 de outubro de 2010 de que a Audiencia Nacional decidira incluír a Resistencia Galega na lista de grupos terroristas.

ANSAmed daba conta da actividade do grupo separatista, ao que se lle atribuía un total de trece ataques desde o inicio de 2010, "sempre co uso de bombas rudimentarias contra empresas inmobiliarias, obras de construción do tren de alta velocidade, sedes de partidos políticos e infraestruturas", describía a información.

Ola con explosivos incautada en Vigo na operación contra Resistencia Galega

A axencia tamén informaba de "ameazas a funcionarios públicos —xuíces, profesores universitarios e a presidenta de Galicia Bilingüe—", o que "motivou que a Audiencia Nacional elevara o nivel de alerta", comunicaba a axencia.

No que se refire aos paralelismos de Resistencia Galega con ETA, ANSAmed salientaba que "ao igual que a *kale borroka*, os mozos simpatizantes de ETA, os membros da organización galega son mozos de grupos de extrema esquerda e *hooligans* de fútbol dos equipos galegos, «manipulados polos veteranos do movemento separatista, que teñen coidado de manterse fóra dos actos violentos», segundo as fontes", explicaba a axencia italiana, que engadía: "Os membros máis antigos da organización son antigos membros do Exército Guerrilheiro do Povo Galego Ceive, un grupo separatista creado en 1986 para importar o modelo da URSS a Galicia, responsábel darredor de 90 ataques e derrotado en 1993. Actualmente existen ao redor de 30 membros rexistrados de Resistencia Galega", máis "segundo as fontes da loita antiterrorista, «hai 200 membros como máximo» en toda a organización", sinalaba ANSAmed.

A axencia de noticias tamén destacaba que "a diferenza de ETA, o movemento separatista galego é marxinal, xa que non ten unha base social que o substente".

O analista Ben West utilizou esta información para aconsellar ao departamento de Análises de Stratfor iniciar un seguimento a Resistencia Galega.

Ataque á sede do PSdeG en Carral

O interese dos analistas de Stratfor nas accións do grupo separatista galego xurdiu tras o atentado contra a sede do PSdeG en Carral con cócteles molotov na madrugada do 18 de xaneiro de 2011.

A vicepresidenta de Marketing Internacional de Stratfor, Antonia Colibasanu, enviou ese mesmo día un correo cunha breve información de Expatica.com na que daba conta dese ataque.

Sete horas despois, West respondía co correo no que copiaba a información da axencia ANSAmed sobre a actividade de Resistencia Galega e no que suxería un seguimento ao grupo separatista ante a expansión das súas accións e o declive de ETA.

Scotland Yard

Na enorme base de datos que creou WikiLeaks cos máis de cinco millóns de correos electrónicos de Stratfor atopamos tamén un documento de Scotland Yard sobre a situación do terrorismo no mundo. Neste documento tamén se dá conta da actividade de Resistencia Galega.

O documento foi creado o 21 de maio de 2007 polo oficial de Intelixencia Tim Anderson. Cinco días despois xa circulaba nas comunicacións privadas de Stratfor. En concreto, estaba en mans de Fred Burton, vicepresidente de Intelixencia da compañía, quen enviou o documento o 22 de maio a unha lista de contactos *vip*, entre os que se atopaban o director executivo e xefe de Intelixencia, George Friedman —fundador de Stratfor— e Don Kuykendall, presidente da xunta da compañía.

Titulado 'Terror Times' ('Tempos de terror'), o documento é un informe semanal do The Metropolitan Police Service Counter Terrorism Command, coñecido tamén como o SO15, creado para protexer a Londres e o Reino Unido da ameaza terrorista.

O informe semanal 'Terror Times' recolle informacións publicadas en distintos medios de comunicación sobre accións terroristas en todo o mundo e pretende ilustrar sobre os métodos e as estratexias empregadas polos terroristas para axudar aos axentes británicos a prepararse para as ameazas do terrorismo actuais e emerxentes, segundo explica o propio Tim Anderson ao comezo deste documento.

Neste caso, trátase do informe da semana do 14 ao 20 de maio de 2007, no que as informacións se dividen en varios apartados: Top stories; General, Internaconal & Internet; United Kingdom, Northern Ireland & Eire, Germany, Netherlands, France, Spain, Italy, Bulgaria, Montenegro, Albania, Greece, Russia, Turkey, Lebanon, Israel, Yemen, Saud Arabia, Kuwait, Iraq, Afghanistan, Pakistan, India, Bangladesh, Nepal, Burma/Myanmar, Thailand, Malaysia, Philippines, Australia, Morocco, Algeria, Ethiopia, Somalia, Nigeria, United States of America, Mexico, Colombia e Peru.

Neste documento, Tim Anderson recollía unha información de thinkspain.com, do 16 de maio de 2006, titulada 'Radical separatists claim responsibility for industrial estate bomb' ('Separatistas radicais reivindican a responsabilidade da bomba nunha nave industrial'). A información facía referencia á desactivación por parte dos TEDAX dun artefacto explosivo no polígono industrial do Ceao, en Lugo. No mesmo texto se informaba tamén de que unha semana antes "o grupo radical Resistencia Galega se atribuíu a responsabilidade da colocación dun dispositivo moi similar nunha obra de construción en Pontevedra".

Como se pode observar en ambos os dous casos —nos correos de Stratfor e no informe de Scotland Yard—, a metodoloxía dos analistas é semellante: recompilar e distribuír internamente informacións publicadas en medios de comunicación que poidan ser de interese para os seus axentes.

Descarga os correos de Stratfor e o documento de Scotland Yard en GC Plus.

ANEXO XI: Publicación 3 de los correos de Stratfor.

"O plan en España é que o Santander tome o control como un banco central"

Nova achega de GC dos correos de Stratfor filtrados por WikiLeaks. Tras anunciarse a nacionalización de NovacaixaGalicia, CatalunyaCaixa e Unnim, o vicepresidente de Análises de Stratfor comentou que "a metade do sistema bancario español é unha absoluta merda" e que o seu rescate levaría ao rescate total do país. Descarga os emails en GC Plus.

- Emails de Stratfor: o plan para o Santander e a "espía" en Moody's
- GC accede aos emails que WikiLeaks filtrou da axencia de intelixencia Stratfor

Por Alberto Quian | Madrid | 31/08/2012 | Actualizada ás 09:00

30 de setembro de 2011. O Banco de España anuncia que o Estado pasa a tomar o control de tres entidades bancarias a través do Fondo de Reestruturación Ordenada Bancaria (FROB) para a súa recapitalización: o 93% de NovacaixaGalicia, o 90% de CatalunyaCaixa e o 100% de Unnim. A noticia percorre medio mundo e os analistas de Stratfor comezan a intercambiarse correos electrónicos. Neses *emails* copian a información que publica ese mesmo día o xornal The Washington Post da axencia Associated Press co título "Spain nationalizes 3 weak banks that failed to meet new capital reserve requirements" ("España nacionaliza tres bancos débiles que non cumprían cos novos requisitos de reservas de capital").

Emilio Botín, presidente do Santander | Fonte: *universia flickr*

Os analistas de Stratfor intercambian opinións sobre a nacionalización dos bancos españois. Nun deses correos —aos que GC tivo acceso a través de WikiLeaks— Peter Zeihan, vicepresidente de Análises da compañía de intelixencia global, é rotundo na súa valoración do sector bancario español: "A metade é unha absoluta merda".

Zeihan xa adianta tamén que a debilidade de boa parte do sector bancario condenará finalmente a España a pedir o rescate total do país; unha eventualidade que a día de hoxe xa se dá por segura e que, posiblemente, se executará este mes de setembro.

O *email* de Zeihan é enviado á conta de correo do departamento de Análises da compañía de intelixencia global. Neste, comenta:

"Aproximadamente a metade do sector bancario español é unha absoluta merda. O seu rescate custaría probablemente o 15-30% do PIB e poñería de cheo a España baixo a tutela do EFSF [Fondo Europeo de Estabilidade Financeira, nas súas siglas en inglés]".

Peter Zeihan, vicepresidente de Análises de Stratfor

En contraposición, Zeihan opina que "por sorte a outra metade [dos bancos españois] é a mellor do mundo". Pero o máis salientábel no seu correo é o seu prognóstico, en *petit comité*, sobre as intencións do plan de continxencia en España, que procuraría asegurar ao Banco Santander como eixo do sistema bancario do país:

> "O plan de continxencia español é literalmente facer que o Santander (a metade desa outra metade) tome o control como o banco central do país", interpreta Peter Zeihan.

Espía en Moody's

Para entender en que nivel se moven Zeihan e os seus colaboradores hai que saber que contan con xente da súa confianza que lles subministra información económica confidencial. Por exemplo, noutros correos aos que tivo acceso GC, Zeihan e o analista xeopolítico Marko Papic falan da presenza dunha "espía" na axencia de cualificación Moody's que colabora con eles. O asunto dos correos electrónicos do 4 de febreiro de 2011 é explícito: "did you ever get an updated bank list from your moody's spy?" ("Conseguiches unha lista actualizada de bancos da túa espía en Moody's?").

Papic, en resposta a Zeihan, contesta:

> "Envieiche os datos totais do sistema bancario + soberanos. Ela estivo demasiado ocupada para conseguirnos os individuais, pero dixo o luns que podería ter tempo para conseguilos esta semana".

Noutro correo do 30 de novembro de 2011, enviado por Zeihan ao correo da sección de Análises de Stratfor co asunto "Standard and Poor's cuts ratings for top US banks" ("Standard and Poor's recorta a cualificación dos principais bancos de Estados Unidos"), o analista responde:

> "Baseándonos na lóxica destas rebaixas, é prudente supoñer que os recortes masivos aos bancos europeos están á volta da esquina".

E xa noutro *email* avisa de que vai recorrer a súa espía para obter información sobre este asunto:

> "Non teño ningunha dúbida de que un feixe tamén está chegando aquí (de feito, dareille un toque á nosa espía en Moody's). As rebaixas de S&P son da institución de novos sistemas, así que case todo o mundo vai ser recualificado aí".

Esa "espía" ben podería ser Liza Hintz, directora adxunta do grupo de investigación de mercados de capitais de Moody's. GC comprobou na enorme base de datos que puxo a nosa disposición WikiLeaks, cos máis de 5 millóns de correos electrónicos de Stratfor, que Marko Papic viña mantendo intensas e constantes comunicacións a través do correo electrónico e do teléfono con Hintz, coa que intercambiaba opinións, informacións e documentos varios sobre asuntos económicos de actualidade relativos á banca española, europea e estadounidense.

Quen é Peter Zeihan?

Peter Zeihan ocupa en Stratfor o cargo de vicepresidente de Análises. A súa labor é supervisar as operacións do día a día do desenvolvemento analítico da compañía e integrar a múltiples fontes de información nunha variedade de produtos para clientes de Stratfor.

A propia compañía de intelixencia preséntao como un "destacado orador, a miúdo perante executivos e inversores en eventos en todo o mundo".

Zeihan uniuse a Stratfor en 2000 e dirixiu varios equipos que traballaban sobre asuntos para Europa, a antiga URSS, América Latina e temas de enerxía.

Foi nomeado vicepresidente de Análises en 2007 e a súa presenza en medios internacionais é habitual: CNN, ABC, Fox News, The New York Times, The Wall Street Journal, Forbes, AP, Bloomberg, MarketWatch, etc.

Antes de unirse a Stratfor traballou para a embaixada de Estados Unidos en Canberra (Australia) e no Centro de Estudos Políticos e Estratéxicos en Washington DC, onde analizaba periodicamente a evolución de Asia, Europa e a antiga Unión Soviética, e facía informes e publicacións para unha variedade de clientes.

Zeihan ten un máster en Desenvolvemento Político e Económico da Patterson School of Diplomacy and International Commerce, un posgrado en Estudos Asiáticos na Universidade de Otago (Nova Zelanda) e unha licenciatura en Ciencias Políticas na Truman State University.

É experto en economía global e xeopolítica, enerxía, gas pizarra, abastecemento de petróleo, produtos alimenticios, demografía global, crise financeira europea, Medio Oriente, China, África, América Latina e Rusia.

Descarga os correos electrónicos de Peter Zeihan en GC Plus.

ANEXO XII: Publicación 4 de los correos de Stratfor.

Os negocios sucios do fretador do 'Prestige'

O xuízo do 'Prestige' comeza nun mes. GC debulla as relacións do responsábel da carga, Mikhail Fridman, oligarca ruso relacionado por Stratfor coa mafia e con crimes como asasinatos e tráfico de drogas.

- Preparando o megaxuízo
- O Prestige a xuízo 10 anos despois
- GC accede aos emails que WikiLeaks filtrou da axencia de intelixencia Stratfor

Por Alberto Quian | Madrid | 13/09/2012 | Actualizada ás 09:00

Ameazas, subornos, extorsións, poxas fraudulentas, tráfico de influencias, tráfico de drogas, prebendas, evasión fiscal, lavado de diñeiro, violencia, asasinatos... O *modus operandi* do magnate ruso Mikhail Fridman baséase en todo tipo de artimañas, intrigas e amaños propios dun corrupto e mafioso para conseguir todo canto se propón nos seus negocios.

Afundimento do Prestige

Así é descrito o oligarca ruso no informe segredo "Mikhail Fridman: Background Investigation" que a axencia de intelixencia global Stratfor realizou no ano 2007 e ao que tivo acceso GC a través da base de datos que WikiLeaks puxo a nosa disposición. En total, 27 páxinas nas que se debullan os negocios e intereses escuros dun home con vínculos co Kremlin e presuntamente involucrado no branqueo de centos de millóns de euros e relacionado co crime organizado: Mikhail Fridman, fundador de Alfa Group, o consorcio que fretou o *Prestige*.

Stratfor cualifícao como un tipo "vil" e vincúlao con asasinatos, tráfico de drogas, branqueo de diñeiro e tráfico de influencias. Nin el nin ningún dos seus socios en Alfa Group e a súa filial Crown Resources serán xulgados pola vertedura do fuel óleo do 'Prestige'. Informe orixinal de Stratfor en GC Plus.

O caso 'Prestige'

No informe de Stratfor existen varias mencións ao accidente do *Prestige*, pero sobre todo debúllanse as relacións e actividades que os responsábeis da carga viñan mantendo nunha serie de negocios escuros. No anexo, titulado "Appendix: Enemies & Investigations" ("Apéndice: inimigos e investigacións"), a compañía dedica un apartado á catástrofe do *Prestige*. Neste, os analistas fan un resumo do accidente e apuntan ás artimañas empregadas para eludir responsabilidades legais :

Mikhail Fridman | Fonte: *Anton Nossik*

> "En novembro de 2002, o *Prestige*, un vello petroleiro cargado con petróleo ruso, partiuse en dous e afundiuse no océano Atlántico. A vertedura ocasionou un desastre ecolóxico cando o fuel óleo cubriu as praias ao longo dun tramo de 125 millas de costa na rexión pesqueira española de Galicia, afectando a aves e outros animais. Crown Resources, unidade de Alfa Group para o transporte de mercadorías con sede en Suíza, era a propietaria da carga do *Prestige*. O fuel óleo cargouse no *Prestige* en San Petersburgo e dirixíase a Singapur, segundo Crown. Crown dixo que ninguén se posicionara para comprar o petróleo.
>
> Crown foi disolta coa fin de minimizar as ramificacións legais".

Alexei Kuzmichev era o máximo responsábel de Crown Resources. É unha das tres persoas ás que Fridman considera tanto un socio como un amigo, segundo explican os analistas de Stratfor. Kuzmichev dirixiu Alfa-Eco, asumiu a presidencia do consello de administración de Russian Technologies e dirixiu entre 1996 e 2002 a petroleira creada en Xibraltar e con sede en Suíza Crown Resources, filial de Alfa Group e propietaria da carga do *Prestige*. Precisamente aquela catástrofe ecolóxica levou a Alfa Group a apartar a Kuzmichev de Crown Resources e a liquidar a empresa para que a catástrofe non salpicara a Kuzmichev nin aos seus socios no consorcio ruso. Así, a finais de 2002 Kuzmichev regresou a Alfa-Eco, que sería rebautizada en 2006 como A1. E Crown Resources sería rebautizada en 2003 como ERC Trading (Energy, Resouces and Commodities) tras a venda de todas as súas accións ao avogado Jost Villiger, ao que algúns consideraron o "home de palla" dos rusos.

Ademais, Stratfor sinala a Alexei Kuzmichev como o membro de Alfa Group "máis involucrado na actividade diaria de lavado de diñeiro do grupo a través de empresas pantasmas internacionais".

Nestas presuntas operacións de fraude, evasión de impostos e lavado de cartos de Alfa Group, Fridman tamén contaría coa colaboración do avogado Norbert Seeger, peza "clave en Alfa", segundo Stratfor, que salienta as "excelentes relacións e os negocios" que mantén "coa familia real de Liechtenstein".

"Suponse, anque non está probado, que [Seeger] proporciona asesoramento amplo a Alfa Group sobre o tema da cobertura legal para a evasión fiscal e as operacións de lavado de diñeiro", especulan os autores do informe.

A conexión Rich

Outra peza clave para entender a trama de Alfa Group-Crown Resources é o comerciante belga de orixe xudeu Marc Rich, quen obtivo a nacionalidade española en 1982, concedida polo ministro de Xustiza de UCD, Pío Cabanillas.

Rich, a quen se relaciona co Mossad —a axencia de intelixencia israelí— estaba moi vinculado a Fridman e o seu consorcio, e o seu nome apareceu na lista de investigados pola catástrofe do *Prestige* como responsábel da carga.

Rich foi fuxitivo do FBI durante case vinte anos por delitos financeiros e por tráfico ilegal de petróleo, e foi dobremente indultado no ano 2001 polo presidente estadounidense Bill Clinton e no ano 2003 polo seu sucesor, George W. Bush. No ano 2001 Rich estivo negociando con Alfa a fusión da súa compañía con Crown Resources, ambas as dúas con sede na cidade suíza de Zug, un auténtico paraíso fiscal. Ademais, un home de confianza de Rich, Steven Rudofsky, que dirixía a firma Marc Rich Investment, pasou en 2002 a Crown Resources como director executivo.

O 5 de febreiro de 2003 Marc Rich Group emitiu unha nota, que reproducimos agora aquí, sobre o caso *Prestige* na que se desvinculaba da catástrofe:

> *Marc Rich Group vese obrigado a publicar a seguinte declaración no que se refire ao 'Prestige' / Crown Resources AG e, deste modo, quere rectificar informes falsos.*
>
> *- O grupo Marc Rich non é o propietario do petroleiro 'Prestige'.*
>
> *- O grupo Marc Rich non é dono da carga do petroleiro Prestige'.*
>
> *- O grupo Marc Rich non vendeu ningunha compañía a Crown Resources AG.*
>
> *- Hai un ano, Marc Rich Group terminou as negociacións con Crown Resources AG con respecto á posíbel venda dunha filial en xuño de 2001 e non se estableceu ningún contacto desde entón.*
>
> *Faga caso omiso de informes contraditorios e non os publique. Grazas.*
>
> *Marc Rich + CO HOLDING GMBH*

Os negocios de Rich e Alfa non son nada claros, cando menos polo que explica Stratfor no seu documento. No informe fálase da súa participación nunha artimaña para favorecerse do programa humanitario "Petróleo por alimentos" que a ONU puxo en marcha entre 1996 e 2003 para Iraq. Rich, xunto con David Chalmers, da compañía Bayoil, "comprou petróleo de Alfa (a través de TNK e Onako) que, a súa vez, tería sido sido adquirido a Iraq", saltándose así o embargo a través de subornos ao goberno de Saddam Hussein (o caso chegou ao Comité de investigación independente do programa Petróleo por Alimentos de Nacións Unidas e, posteriormente, a xustiza suíza suspendeu a investigación por falta de probas).

Rich é un home con moitos vínculos e amizades poderosas en España. Por exemplo, co empresario vigués e directivo do Real Madrid, Fernando Fernández Tapias, quen compartiu negocios con Rich en Brasil no sector do aluminio. Tapias era, precisamente, o dono dos remolcadores que levaron ao *Prestige* mar adentro antes de afundirse, e foi un dos persoeiros que enviou a Clinton unha carta solicitando o indulto de Rich. Nesta trama para salvar o pescozo de Rich tamén estaría implicado o rei Juan Carlos I, do que se comentou en varios medios que tamén intervira directamente para conseguir o seu indulto.

Alfa e o negocio do petróleo

Mikhail Fridman meteuse de cheo no negocio do petróleo a finais dos anos 90. Foi a través dunha intriga política a mediados daquela década, cando o presidente Boris Yeltsin recibiu a axuda económica dos oligarcas do país ante a *ameaza* dos comunistas de cara ás eleccións. A cambio, Yeltsin puxo en mans dos magnates, a través de novas poxas fraudulentas, os restantes bens que aínda mantiña o Estado ruso, segundo o relato dos analistas. Así, Alfa-Bank logrou adquirir por só 810 millóns de dólares o 40 por cento de TNK, que logo se convertiría na xoia da coroa do imperio Alfa. A través doutras manobras nos meses seguintes, Alfa Group e Access-Renova repartíronse o 50% da compañía petroleira. No 2007 o seu valor estimábase en 8.000 millóns de dólares.

Crown Resources

Entre os activos de Alfa Group, o informe de Stratfor sinala a súa "plena propiedade" de Crown Resources, a empresa comercial con sede en Suíza especializada na venda en Europa Occidental de petróleo ruso e produtos derivados deste, ademais de intereses no sector do aluminio. No documento se destaca que Crown Resources xestionaba a maior parte do comercio do Grupo Esparto e a súa propia filial, Crown Trade and Finance, con sede no paraíso fiscal das Illas Virxes Británicas.

Porén, oficialmente Crown Resources levaba case a totalidade das súas finanzas e dos seus ingresos a través da empresa pantasma ERC Trading coa fin de minimizar os vínculos formais co Grupo Esparto, encargado da evasión de impostos e lavado de diñeiro de Alfa Group, segundo se indica no informe.

Esparto non seria a única entidade escura creada por Alfa Group. Entre as súas filiais atópase, por exemplo, Alfa Capital Markets, que "basicamente serviu como vehículo para o lavado de diñeiro e o fraude en Estados Unidos nunha ida e volta do capital a Rusia para defraudar e, finalmente, tomar o control do mercado de móbiles da Federación Rusa", explícan os especialistas da axencia norteamericana. De feito, IPOC Growth Fund International emprendeu demandas federais por crime organizado en 2006 contra a filial de Alfa Group e o seu xerente nos Estados Unidos, Leonid Rozhetskin.

Alfa Group

As orixes de Alfa Group atópanse na extinta Unión Soviética e na venda de entradas para espectáculos teatrais. Daquela, todos os billetes para o teatro estaban reservados expresamente aos membros do Partido Comunista. Se non se tiña un enlace directo con algún destes, o único xeito de acceder aos eventos culturais rusos era a través dalgún intermediario que fose quen de conseguir e revender entradas que non se ían utilizar, o cal era ilegal. Fridman cumpriu ese papel de revendedor, ofrecendo a outros as entradas dos membros do partido que non as necesitaban.

Cando o primeiro ministro soviético Mikhail Gorbachev aprobou unha serie de reformas económicas aperturistas para o fomento da empresa privada, Fridman e os seus compañeiros do Instituto Estatal de Moscova de Aceiro e Aleacións crearon unha cooperativa de entrega de mercancías e outros servizos. En 1988, creou a súa propia cooperativa, Alfa Foto, e posteriormente, Alfa-Eco, unha empresa de comercio de produtos básicos coa que conseguiu o capital para crear Alfa-Bank en 1991.

Como recolle o informe de Stratfor, a firma financeira Renaissance Capital chegou a cualificar a Alfa como o "conglomerado máis agresivo en Rusia", salientando o seu uso de "métodos hostís" tanto para a compra de activos como para a súa venda.

Perfil de Mikhail Fridman

O informe de Stratfor é contundente no que se refire ás artimañas políticas e económicas de Mikhail Fridman. Na introdución dise que "Fridman foi un dos orixinarios oligarcas rusos que roubaban ao cego Estado ruso na década de 1990". Tamén se di que "é un dos poucos daqueles [oligarcas] que non están mortos, exiliados ou no cárcere".

Fridman é un tipo de "poucos amigos" e "moitos inimigos" que coinciden, todos eles, en cualificalo como un tipo "astuto, áxil, evolucionado, paciente, calculador, vengativo, combativo e, sobre todo, subestimado".

O documento de Stratfor describe a un Fridman "moito mellor estratega política e económicamente que os seus poderosos rivais", conseguindo sempre "esmagar aos seus inimigos". Os seus aliados salientan del a súa "impecábel perspicacia para os negocios, o seu mal xenio e a súa absoluta ausencia de apego emocional nos negocios". Rasgos da personalidade que, din, son claves no seu éxito como home de negocios.

De feito, Stratfor auguraba neste documento que Mikhail Fridman acabaría sendo o "oligarca máis poderoso de Rusia" grazas á diversificación dos seus investimentos a través da todopoderosa compañía Alfa Group, responsábel do petróleo que verteu o *Prestige* na costa galega e que ocupa un dos máis destacados lugares na economía rusa, sendo un conglomerado financeiro-industrial con intereses enerxéticos no petróleo e no gas natural, no comercio de produtos básicos, na banca comercial e de inversión, seguros, telecomunicacións, metais, alcol, supermercados...

Orixes

Mikhail Maratovich (Misha) Fridman naceu o 21 de abril de 1964 nunha familia xudía de clase media en Lviv, Ucraína. Pertencentes ao Partido Comunista, traballaban como enxeñeiros na industria armamentística soviética. En 1986, Fridman graduouse con altos honores no Instituto de Moscova de Aceiro e Aleacións.

"Ao igual que moitos oligarcas de Rusia, Fridman considérase primeiro xudeu e nun segundo e distante lugar, ruso", describe Stratfor no seu informe, no que se destaca o "desprezo" que o magnate sente polos rusos: "No caso Fridman, porén, definitivamente hai unha escura raia. Despreza aos rusos e parece que gozou perversamente co papel que desempeñou na crise económica de Rusia durante a década de 1990. Non ten reparos morais á hora de defraudar aos rusos e as súas accións indican que non ten problema en estafar a ninguén".

Segundo Stratfor, a filosofía para os negocios de Fridman ten unha raizame familiar, "particularmente na súa avoa", dona dunha tenda de utensilios de cociña en Lviv, Ucraína, onde Fridman creceu, aclara a compañía estadounidense. "O seu consello para os negocios era simple: «Nunca hai que tratar cos comunistas»", explícase. Por iso, Fridman sempre tentou manterse "á marxe dos debates políticos nacionais" e "foi un dos primeiros oligarcas rusos en procurar un consenso co goberno de Putin". Os analistas de Stratfor lembran que a principios do ano 2000 Vladimir Putin chamou a todos os oligarcas ao Kremlin e ofreceulles un trato: deixar de roubar, pagar os seus impostos e permanecer fóra da política a cambio de que o Estado os deixase en paz. "Fridman aceptou con entusiasmo a oferta, mais o ex-director executivo de Yukos, Mijail Khordokovsky, non. Fridman, finalmente, foi quen de utilizar o patrocinio estatal para selar a fusión internacional da súa empresa petroleira (TNK) coa multinacional BP co obxectivo de crear TNK-BP; Jodorkovski está en quebra e no cárcere", comparan os analistas.

Cunha traxectoria meteórica, Fridman chegou a ser presidente da xunta directiva do consorcio Alfa Group —propietario da carga do *Prestige*—, presidente do consello de administración de Alfa-Bank, e presidente da xunta directiva da empresa enerxética TNK-BP. Malia este perfil de tipo poderoso, Fridman "prefire manter un perfil baixo en termos de economía, política e vida persoal", sinalan os analistas, que engaden: "Porén, iso non se traduce nunha vida austera. Ten un bo número de casas palaciegas en toda a antiga Unión Soviética e o seu apartamento de Moscú crese que ten máis de 3.600 metros cadrados".

Entre as súas afeccións máis notábeis inclúense "as armas e o coleccionismo de arte, amosando unha inclinación pola arte extremadamente cara, como obras de Picasso", apúntase no informe.

Un estratega agresivo

Segundo Stratfor, Fridman acostuma actuar "por cobiza, non por ego ou por unha necesidade de vinganza. Pero se se enfurruña nun proceso de adquisición ao que non vai renunciar, vai asegurarse de que determinadas persoas sexan completamente arruinadas".

O infome da compañía de intelixencia global insiste en describir a Fridman como un tipo que "se move agresivamente contra calquera activo que desexe conseguir, e faino por cobiza, non por ego".

Os propios socios comerciais de Fridman describen ao magnate ruso como un tipo "profesional, esixente, corrupto e vil".

"Conceptos tales como a honestidade e a transparencia non só se perden en Fridman", senón que ademais "os evita deliberadamente", dise no dossier, no que se apuntan algúns ataques de natureza financeira, xurídica e física que presuntamente acostuma a poñer en práctica Alfa Group para conseguir os seus obxectivos. Así, entre outras tácticas, se salienta a suposta concesión de préstamos abusivos a través de Alfa-Bank para logo facerse co control das empresas prestatarias quebradas a un prezo menor do mercado, os subornos de xuíces ou o uso de "matóns armados" para, por exemplo, facerse coas accións que tiñan algúns traballadores de determinadas empresas rusas aos que o Goberno lles concedera esas partipacións no proceso de privatización dos anos 90 en Rusia.

Stratfor tamén acusa a Alfa Group de ter procurado regularmente a axuda explícita do goberno ruso para as súas operacións. Un bo exemplo disto, sinalan os analistas, foi o chamamento que Fridman lle fixo a Vladimir Putin para arranxar a fusión entre a petroleira rusa TNK e a británica BP no ano 2003.

Fridman é descrito como un home sen principios éticos e tamén como un tipo receoso que "non ten ningunha intención de revelar o funcionamiento interno dos seus activos, non só por codicia ou para protexerse do escrutinio legal, senón tamén por simple medo", aducen os analistas, que observan que estes receos son comúns entre os oligarcas rusos, xa que "os seus imperios foron creados polo tráfico de influencias, poxas fraudulentas de privatizacións, fraude, roubo, malversación, evasión de impostos, brutalidade, corrupción e manipulación do sistema legal", enumera o informe.

Fridman veríase a si mesmo como un inversor que "está absolutamente disposto a abandonar sen pensalo unha liña de negocio que non funcione, e non ten intención de dominar ningún sector en particular". Por exemplo, "a súa meta de construír un imperio de comunicacións móbiles baséase na ambición de gañar accións nunha importante empresa global de telecomunicacións de celulares, non porque procure un nicho de mercado ou un monopolio para el. Se un obxectivo resulta particularmente resistente aos seus esforzos, simplemente segue adiante".

Como se recorda no informe, o propio Fridman dixo que algún día Alfa Group se retiraría do negocio do petróleo e da banca para investir noutros activos. O seus obxectivos son sempre "a eficiencia, o crecemento e a maximización do valor da empresa a longo prazo", mais isto "non quere dicir que o beneficio non sexa tamén unha preocupación fundamental". Mais, como sinala Stratfor, Fridman ten transferidos moitos fondos en paraísos fiscais para "maximizar os seus ingresos e minimizar os impostos do goberno", e poder así tamén "dispoñer deses cartos para investimentos e adquisicións, segundo sexa necesario", coméntase no documento.

Stratfor agrupa aos principais empresarios rusos en dúas categorías: os tácticos e os estrategas. Os primeiros son empresarios que "procuran calquera vantaxe que cren que lles vai beneficiar no curto plazo" e teñen a "típica mentalidade rusa do saqueo", sinala o informe.

No caso de Fridman, Strafor inclúeo no grupo dos estrategas, que se ben se asemellan aos tácticos na "utilización de técnicas sen restricións éticas", estes teñen unha visión a máis longo prazo dos seus negocios. "A maioría dos estrategas", explica Stratfor, "quere investir as súas ganancias nas súas empresas para máis tarde poder vender os seus activos por un prezo máis alto".

"Fridman só inviste en proxectos nos que pensa que ten posibilidades de obter enormes ganancias. Combina iso coa falla dun compás moral", descríbese no informe.

Seguridade

Segundo os analistas de Stratfor, "Fridman mantén o seu propio grupo de seguridade e os seus compañeiros executivos de Alfa actúan en moitos aspectos como unha pequena forza policial". Mais por ese perfil público baixo que teima en manter, Fridman pensa que "ten asegurada a súa seguridade persoal".

"Desde os tempos turbulentos da década de 1990, Fridman foi recortando o seu séquito persoal e agora rara vez leva máis de dous ou tres escoltas visíbeis. A súa axenda é suficientemente caprichosa como para non dar tempo a examinar os lugares públicos aos que acode, na súa maioría clubes de jazz, antes da súa chegada", clarifica o documento.

Ese desexo por manter un perfil público máis baixo que os demais oligarcas rusos esténdese aos medios de comunicación. Se para os homes máis poderosos do país os medios de comunicación rusos son parte do escenario no que competir para "darlle forma aos seus imperios corporativos e difamar aos seus opoñentes", Fridman parece preferir ignorar á prensa e manter unha postura menos entremetida neste sector. "Esta decisión parece que o beneficiou, xa que o goberno incrementou o seu control en todos os medios de comunicación durante os últimos cinco anos", explícase.

Pyotr Aven, o cerebro

Durante a década dos 90 Fridman participou con outros oligarcas-cleptócratas rusos en poxas amañadas para facerse por un valor mínimo con moitas empresas estatais, o que acelerou o colapso económico ruso. Nesta época, no ano 1994, conectou con Pyotr Aven, "o seu primeiro e máis importante aliado", aclara Stratfor. Aven formaba parte dos reformadores idealistas rusos. Foi ministro de Comercio Exterior entre 1991-1992 e representante de Rusia no G-7, coincidindo co goberno do primeiro ministro Yegor Gaidar, "o primeiro goberno postsoviético verdadeiro da Federación Rusa", din os analistas de Stratfor, que sinala a Aven como un dos burócratas que establecereon as condicións para as poxas amañadas nas que participaron os oligarcas.

Aven, propietario da colección de arte rusa máis grande do país, pasou a formar parte do consello de administración de Alfa Group, foi presidente de Alfa-Bank até xuño de 2011 e é o presidente de Alfa Banking Group e AlfaStrakhovanie Group, unha das maiores aseguradoras de Rusia, ademais de co-presidente da compañía de medios de comunicación CTC Media Inc.

Stratfor sinala a Aven como "o cerebro detrás das estratexias de Alfa e máximo responsábel das súas operacións diarias, mentres Fridman serve tanto como o rostro das operacións, como negociador carismático e astuto que pecha os acordos". En definitiva, Pyotr Aven é o "cerebro de Alfa"; o "contable e economista detrás do escenario que fai que todo funcione"; o home que "conta coa amizade de Putin"; o "director xeral de Alfa e a cara que proporciona unha dirección estratéxica", describen os analistas da axencia estadounidense.

Aven non é un tipo limpo, segundo Stratfor. "Está involucrado ao máximo en todos os negocios de Fridman e como xerente operativo ten máis coñecemento das actividades ilegais cuestionábeis ou indiscutíbeis que o propio Fridman", elucida o informe. Stratfor mesmo recorda que o grupo de traballo contra a corrupción rusa do Tribunal de Distrito de Columbia, en Estados Unidos, sinalouno como "actor en diversos actos de corrupción, incluído o tráfico de drogas".

A través dos vínculos de Aven con Putin, Fridman tamén accedeu a outro aliado fundamental para os seus negocios: o ex-primeiro ministro Mikhail Fradkov. Fradkov traballou para Alfa e "débelle lealdade a Aven", din os analistas, que especifican que o ex-primeiro ministro chegou ao goberno ruso "en parte debido á aprobación de Putin da fusión TNK-BP".

As outras dúas pezas claves

O triunvirato que domina Alfa Group e para o que traballa Pyotr Aven complétase con German Khan e Alexei Kuzmichev, co-fundadores do consorcio con Fridman.

German Khan é un vello amigo de Fridman. Coñecéronse no Instituto Estatal de Moscova de Aceiro e Aleacións e é o director executivo de TNK. Entre os seus *méritos* está, por exemplo, que "foi clave na toma de control de Yugraneft, da empresa canadense Norex, e nas ameazas explícitas e subornos ao director executivo de Norex, Alex Rotzang, e á directora xeral de Yugraneft, Lyudmila Kondrashina", dise no informe.

Khan tamén é membro dos consellos de administración de Alfa Finance Holdings, grupo industrial e financeiro con sede en Bulgaria, e Slavneft, unha "empresa petroleira estatal da que Alfa Group adquiriu unha participación do 50 por cento nunha poxa amañada no 2002", esclarece Stratfor.

Alexei Kuzmichev é a outra persoa de confianza de Fridman desde os anos de universidade. Como xa vimos, entre outros cargos de máxima responsabilidade, Kuzmichev dirixiu entre 1996 e 2002 a empresa petroleira Crown Resources, filial de Alfa Group e propietaria da carga do *Prestige*. Tras a traxedia ecolóxica e económica para Galicia, e o impacto mediático e político que tivo non só a nivel nacional, senón tamén internacional a catástrofe, nos despachos de Alfa Group se decidiu apartar a Kuzmichev de Crown Resources e liquidar logo a empresa para eximir de responsabilidades a Kuzmichev e, polo tanto, a Fridman e o seu consorcio.

Relacións co Kremlin

A influencia económica de Alfa Group en Rusia non é unha preocupación para o Kremlin, segundo os analistas de Stratfor. A aparente ausencia de aspiracións propiamente políticas de Fridman e os seus socios fai que "o equipo de Putin pareza disposto a pasar por alto as indiscrecións de Fridman e Aven", comentan os expertos en intelixencia da compañía estadounidense, que proseguen: "Á vista do Kremlin, Fridman e Aven son dous ladróns e mentirosos, pero están entre os [oligarcas] máis respectuosos e construtivos". E nisto tivo un papel fundamental Pyotr Aven, quen "fai todo o posíbel para que Fridman non lle pise os pés ao Kremlin", explícase no dossier.

Stratfor fala de que é o propio Putin o interesado en "non compartir ninguna relación persoal ou profesional con Fridman". Porén, "Aven e Putin considéranse amigos íntimos e confidentes o un do outro", prosegue o informe.

Con quen si mantivo unha estreita relación Fridman foi con Vladislav Surkov, o actual viceprimeiro ministro ruso, considerado o auténtico ideólogo do Kremlin, co que Fridman tamén coincidiu no Instituto Estatal de Moscova de Aceiro e Aleacións a principios da década dos anos 80. Xa a principios dos 90 Surkov estivo traballando en Alfa-Bank como vicepresidente, pero acabou traizoando a confianza de Fridman. "Surkov xa fixera amizade con Putin durante a súa primera presidencia e ía ser nomeado xefe de comercio en Transnefteprodukt [empresa enerxética] por prover información negativa de Fridman. Pero en vez de Transnefteprodukt, Surkov apartouse para executar a campaña electoral de Putin, que o levou a converterse no seu principal asesor", explican os analistas. Segundo estes, coa incorporación de Surkov ao círculo máis íntimo de Putin, Fridman e Aven retomaron as conexións con este, se ben estas novas relacións tiñan unha única finalidade: "Surkov dille a Fridman precisamente o que ten que facer para permanecer fóra da lista de golpes do Kremlin ou para asegurarse a asistencia do Kremlin nunha batalla comercial, e Fridman cumpre completamente", dise no documento.

Destas novas relacións naceu Patriot Capital baixo o auspicio de Alfa Group para "facilitar os investimentos no sector da defensa rusa", esclarecen os autores do informe.

Ademais, Alfa Group ofreceu un "forte apoio financeiro" á organización política xuvenil Nashi, "unha das novas ferramentas políticas do Kremlin para asegurar a lealdade política a nivel nacional, e que representa claramente unha reacción á Revolución Laranxa de 2004 en Ucraína, na que os movementos xuvenís foron fortes impulsores", recórdase. Este apoio de Alfa Group a Nashi sería unha das súas respostas aos ditados de Surkov, quen "tomou un papel activo na conformación da organización do grupo e da súa ideoloxía desde o ano 2005", coméntan os expertos.

Estas novas relacións con Surkov son un síntoma máis do que Stratfor sinala como a característica más importante de Fridman: a súa "adaptabilidade" a cada goberno e conxuntura para "asegurar a súa fortuna e a súa vida".

Uso da violencia

Stratfor considera que Fridman utiliza tres tipos de violencia coa fin de conseguir algúns dos seus obxectivos.

O primeiro é o "fortalecemento da violencia política en mans do Estado". Como xa vimos, Fridman financia á organización xuvenil Nashi, segundo informacións proporcionadas polos líderes deste movemento que falaron cos axentes de Stratfor.

En segundo lugar, Stratfor afirma que Fridman está estreitamente ligado, a través da financiación de Alfa, á organización moscovita Solntsevo (Solsnetskaya), "unha das maiores e máis poderosas asociacións rusas de crime organizado", involucrada no tráfico de drogas, extorsións, lavado de diñeiro e subornos. "A organización está dirixida por Sergei Mikhailov, considerado como un dos mafiosos máis perigosos e notorios en Rusia", esclarecen os analistas de Stratfor, cuxas fontes sinalan que "todas as evidencias que involucran a Fridman e Aven con este grupo foron oficialmente eliminadas de todos os rexistros".

Segundo Stratfor, Fridman e Aven xa tiñan relacións con Solsnetskaya na década dos anos 90, cando xa utilizaban a membros desta organización para a súa protección e cos que mesmo fixo negocios. Mesmo se fala de que Aven asesorou aos membros de Solsnetskaya nos seus negocios no tráfico de drogas a escala mundial. "En concreto, Alfa Group está involucrado no transporte de drogas do sudeste de Asia a través de Rusia cara Europa, o lavado de diñeiro dos carteis da droga colombianos e no suborno de órganos da xustiza en Rusia", relátase no documento.

O informe vai máis aló e vincula a Fridman con varios asasinatos en Rusia (o terceiro método de violencia). Malia que oficialmente Fridman nunca foi vinculado a ningún crime, "crese que é, polo menos, parcialmente responsábel de moitos dos asesinatos que afectan á sociedade rusa, en particular de xornalistas", denúnciase no informe, no que se argúe que precisamente este poder de intimidación é o que lle permite a Fridman "gozar dun historial tan limpo".

Stratfor pon como exemplos o asasinato no ano 2000 do xornalista ucraíno Georgi Gongadze no seu país e o do xornalista estadounidense Paul Klebnikov en Moscova no ano 2004, sobre os que Stratfor puido "corroborar parcialmente" a relación do magnate ruso nestes crimes tras consultar a varios xornalistas e políticos de Ucraína.

No caso de Gongadze, críase que estaba investigando os vínculos entre Fridman (a través de Alfa Group) e o líder do Partido Socialista ucraíno Oleksandr Moroz. "Supostamente, Moroz prometera a Alfa varios proxectos de enerxía lucrativos no caso de ser elixido presidente de Ucraína. De acordo coas testemuñas no caso, Alfa contratou á banda local de crime organizado Izmailovskaya para asasinar e decapitar a Gongadze coa fin de acalar as súas investigacións", explican os analistas de Stratfor.

Pola súa banda, Klebnikov era un xornalista da edición rusa de Forbes e estaba investigando unha serie de actividades de Alfa Group cando foi asasinado. "Un funcionario dentro do círculo íntimo de Putin díxolle a Stratfor que antes da súa morte Klebnikov estaba investigando as actividades de Alfa respecto a IPOC, Megafon e o petróleo de Acerbaixán", aclárase no documento da compañía de intelixencia norteamericana.

Con todo, nin Fridman nin ningún dos seus socios de confianza foron nunca condenados por ningún delito. No caso do *Prestige* tampouco se sentarán no banco dos acusados.

Descarga en GC Plus do documento orixinal de Stratfor: "Mikhail Fridman: Background Investigation".

Mikhail Fridman | Fonte: *Anton Nossik*

Sergei Mikhailov, líder da mafia rusa Solntsevskaya Bratva, que Stratffor relaciona co fretador do Prestige

ANEXO XIII: Publicación 5 de los correos de Stratfor.

España xa advertiu do "enorme poder" de Alemaña na UE

Nova achega dos correos de Stratfor. Camilo Villarino, conselleiro para Asuntos Transatlánticos e de Seguridade e Defensa na Embaixada de España en Washington, advertiu en comunicacións segredas cos analistas de Stratfor dos perigos do novo sistema de votación no Consello da UE, que dará a partir do ano 2014 un "enorme poder" aos "catro grandes": Reino Unido, Francia, Italia e, sobre todo, a Alemaña. A crítica contrasta coa subordinación de España aos ditados económicos que chegan dende Berlín.

› GC accede aos emails que WikiLeaks filtrou da axencia de intelixencia Stratfor

Por Alberto Quian | Madrid | 05/11/2012 | Actualizada ás 09:00

"A cantidade de poder que o novo sistema transfire aos 'catro grandes' países da UE, e en particular a Alemaña, é enorme". Esta era a advertencia que o diplomático español Camilo Villarino facía sobre o sistema de votación do Consello da Unión Europea nun dos correos electrónicos que intercambiou con Marko Papic, analista xeopolítico da axencia de intelixencia global Stratfor.

Rajoy e Merkel, líderes de España e Alemania nunha convención de conservadores europeos | Fonte: *EPP Flickr*

Nun *email* enviado o 24 de marzo de 2010, Papic agradecía a Villarino a súa "concienciuda e expansiva" resposta, "extremadamente valiosa" para os analistas de Stratfor. E aseguráballe que toda a correspondencia entre ambos os dous era *off the record*. "Con Stratfor sempre o é", garantíalle.

Agora, grazas á base de datos que WikiLeaks puxo á nosa disposición, podemos coñecer as consideracións do diplomático español —conselleiro para Asuntos Transatlánticos e de Seguridade e Defensa na Embaixada de España en Washington— sobre temas que están a afectar en profundidade á nosa sociedade. O propio Villarino explicaba a Papic, "*off the record*", as súas consideracións sobre un asunto que é "máis importante do que a xente cre", apuntaba o diplomático español.

Villarino contestara a unha petición de Papic, do 18 de marzo, para coñecer a postura de España respecto do cambio do sistema de votación dos Estados no Consello da UE, que entrará en vigor o 1 de novembro de 2014.

"Estaría moi interesado en coñecer a súa opinión e visión sobre o proceso de negociación do Tratado de Lisboa. Cal foi a posición española sobre o aumento do peso da poboación?", escribiulle Papic a Villarino.

Camilo Villarino, diplomático español.

Noutro correo anterior, do 16 de marzo, Villarino suxeriu a Papic que lle botara un vistazo ás consecuencias do novo sistema de votación previsto no Tratado de Lisboa. "Este novo sistema de votación incrementará notablemente o poder de Alemaña na Unión Europea", adiantaba o diplomático español, quen salientaba: "Seino ben: pasei oito anos negociando os novos tratados da Unión Europea".

Camilo Villarino intercambiou varias comunicacións con Stratfor dende a súa conta de correo oficial do Ministerio de Asuntos Exteriores e de Cooperación español, e asinou eses correos cos seus datos oficiais como membro da diplomacia española:

> Camilo Villarino-Marzo
>
> Political Counselor
>
> Embassy of Spain
>
> 2375 Pennsylvania Ave., N.W.
>
> Washington DC 20037
>
> Tel. 202.7282351
>
> Fax 202.8335670

A continuación publicamos en varios apartados o correo íntegro de Villarino.

A posición de España

"España opúxose constantemente ao novo sistema, coñecido coloquialmente como 'Dobre maioría' (xa que require unha maioría de Estados membros e unha maioría da poboación), dende que esta proposta apareceu, a principios de 2003, na Convención Europea que redactou o Tratado Constitucional da UE, ata a chegada ao poder de José Luis Rodríguez Zapatero (aínda que nos últimos meses do mandato de José María Aznar España mostrou un certo grado de flexibilidade nesta materia, incorporando ao novo sistema de voto varias enmendas). O mesmo fixo Polonia. Ambos os dous países, como explicarei máis tarde, ían perder máis co novo sistema. O principal defensor do novo sistema de votación foi o presidente da Convención, Valery Giscard d'Estaing. Os grandes beneficiarios foron (e son), máis que nada, Alemaña e, nunha categoría separada, Reino Unido, Francia e Italia. Lixeiramente, tamén os Estados membros máis pequenos dalgún xeito aumentaron a súa cota de poder (debido á necesidade de contar con polo menos a metade dos Estados membros para acadar un maioría cualificada)".

Explicación do sistema de votación

"Antes de continuar teño que explicar como funciona o sistema de votación actual ('actual', xa que estará en vigor ata 2014 e na práctica, ata abril de 2017). O actual sistema, coñecido como o 'sistema de Niza', está baseado nun sistema de 'voto ponderado', no que cada Estado membro ten un certo número de votos en función de varios criterios políticos (que non aparecen en ningures nos Tratados da UE e son en gran medida o resultado do puro 'poder' de negociación) como o PIB, a poboación, a 'posición internacional', o comercio internacional, etc. Este sistema de voto ponderado foi utilizado dende as orixes das entón Comunidades Europeas, nos anos 50. O número de votos asignados aos distintos Estados membros experimentou cambios ao longo dos anos, sobre todo debido ás ampliacións.

No sistema actual, Alemaña, Francia, Reino Unido e Italia (os 'catro grandes') teñen cada un 29 votos; España e Polonia teñen cada un 27 votos; logo veñen Rumania, con 14 votos, e os Países Baixos, con 13 votos; e logo un grupo de países, como Bélxica, Portugal, Hungría ou a República Checa, con 12 votos, etc. Os Estados membros máis pequenos, por exemplo como Luxemburgo, teñen 4 votos. Coa fin de acadar unha maioría cualificada, hai a necesidade de contar co apoio dos Estados membros que representen polo menos 255 votos dun total de 345 (o que significa que calquera que poda reunir 91 votos ten unha 'minoría de bloqueo': trátase dun concepto clave que vou tratar máis adiante). É certo que o Tratado de Niza di que tamén necesitas contar co apoio da metade dos Estados membros da UE e que teñen que representar polo menos o 62% da poboación da UE, pero en termos matemáticos a distribución de votos é tal que dos 134 millóns de combinacións posibles de voto só existen 23 exemplos, dentro da actual Unión Europea de 27 Estados membros, onde este non é o caso, polo que na práctica se pode facer caso omiso desoutros criterios e só considerar os votos.

Este 'sistema ponderado' sempre tivo como unha das súas principais características o feito de que 'prima' aos Estados pequenos: canto máis pequeno es, máis grande é a 'prima'. Luxemburgo ten unha poboación 200 veces menor que Alemaña, pero a diferenza no poder de voto en termos absolutos é lixeiramente máis grande que 1 a 7. O mesmo ocorre con todos os Estados membros. O propósito deste sistema foi conceder a cada Estado voz e voto propio nos asuntos da UE. Tamén favorece que os Estados membros formen alianzas diferentes para constituír unha 'minoría de bloqueo' e forzar a continuación das negociacións.

No caso de España, isto significa que xunto con Polonia suman 54 votos. Aínda terían que conseguir 37 votos para acadar unha 'minoría de bloqueo', pero poden buscalos en toda unha serie de socios (en moitos casos serían suficientes outros catro Estados membros)".

O novo sistema de dobre maioría

"Todo isto vai cambiar co novo sistema de 'dobre maioría', no que a dobre maioría se forma cando se ten o apoio dos Estados membros que representan o 65% da poboación da UE e polo menos o 55% do número dos Estados membros (estou simplificando, pero estes son os fundamentos). Necesitas o 35,01% da poboación da UE para 'bloquear' a adopción dunha lexislación que consideres contraria aos teus intereses: España e Polonia, para continuar co exemplo anterior, representan aproximadamente o 17% da poboación da UE; para obter outro 18% necesitas o apoio de polo menos un dos 'catro grandes' (esta é a clave do novo sistema) ou tes que pensar no 'bloqueo' a través do número de Estados membros que se opoñen á decisión en cuestión (unha tarefa case imposible). A cantidade de poder que o novo sistema transfire aos "catro grandes", e en particular a Alemaña, é enorme.

Por que só España e Polonia se opuxeron ao novo sistema, até que cederon? Dado que a maioría dos outros 'perdedores' eran demasiado novos no xogo para atreverse a xogar duro (todos os recén chegados o 1 de maio de 2004, agás Polonia [Chipre, Eslovaquia, Eslovenia, Estonia, Hungría, Letonia, Lituania, Malta e República Checa]) ou pensaban que tiñan que concentrar os seus esforzos na reserva dunha nacionalidade na Comisión Europea (que finalmente conseguiron), mentres que os polacos e españois se fixeron cargo dos seus intereses na 'batalla' das votacións o mellor que puideron. Non esqueza que o mantemento dun comisionado foi sempre tamén un obxectivo nacional principal nas negociacións para moitos Estados membros: a Comisión Europea ten case o poder exclusivo de presentar propostas lexislativas, as cales, se existen divisións entre os comisarios, poden ser adoptadas pola xunta por unha maioría simple, ademais de que no proceso lexislativo da UE o Consello (os Estados membros) só pode modificar unha proposta da Comisión co seu consentimento ou por unanimidade".

Camilo Villarino: conselleiro para Asuntos Transatlánticos e de Seguridade e Defensa na Embaixada de España en Washington. Entre 2002 e 2008 foi subdirector xeral de Asuntos Institucionais para a Unión Europea no Ministerio de Asuntos Exteriores, responsable do equipo técnico encargado das negociacións dos novos Tratados da Unión Europea. É, ademais, vicepresidente do Real Instituto de Estudos Europeos. É autor do libro 'Un mundo en cambio. Perspectivas de la política exterior de la Unión Europea'.

ANEXO XIV: Publicación 6 de los correos de Stratfor.

Os negocios de España na guerra libia

As grandes empresas españolas comezan a recoller os froitos da intervención de España no conflito libio. GC publica os correos electrónicos confidenciais do diplomático español Camilo Villarino con Stratfor e un informe desta axencia de intelixencia nos que se explican os intereses comerciais e xeoestratéxicos dos países europeos implicados na guerra que acabou co réxime de Muamar Gadafi en 2011.

Por Alberto Quian | Madrid | 10/01/2013 | Actualizada ás 08:00

O pasado 17 de decembro, unha delegación española composta por representantes de 16 empresas e os ministros de Exteriores e de Fomento, José Manuel García-Margallo e Ana Pastor, visitou Libia para "tender pontes" económicas co país norteafricano. Foi o primeiro desembarco empresarial trala caída do goberno de Muamar Gadafi en 2011 e a designación en novembro pasado do novo Goberno libio.

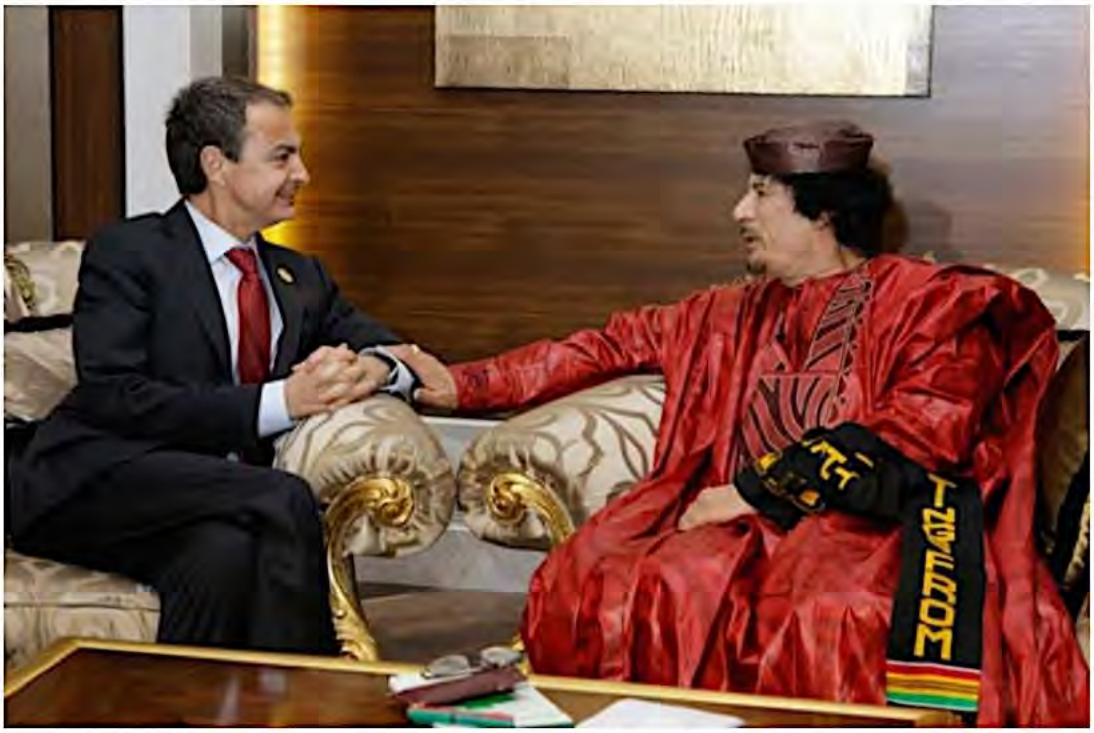
Camilo Villarino, diplomático español.

A Libia viaxaron delegados das principais empresas españolas. Repsol, Indra, Gas Natural, Cobra, Abengoa, Asfibe, Sacyr, Aries Ingenieros y Sistemas, Grupo Puentes y Calzadas, Idom, Isolux, Sercobe, Rover Alcisa, Ingecons, Anci e M. Torres Olvega son as primeiras compañías do Estado que agora procuran sacar tallada da destrución do país africano trala guerra, que rematou en outubro de 2011 coa morte de Gadafi, despois de oito meses de contenda fratricida na que Europa meteu as súas gadoupas nunha intervención militar liderada primeiro por Francia, Reunido Unido e Estados Unidos, e soportada logo pola OTAN.

Agora, máis dun ano despois da fin do conflito, os europeos comezan a recoller os froitos da súa intervención en forma de contratos millonarios. A guerra en Libia tivo, como todas as guerras modernas, moito de negocio. Así o recoñecía no seu momento o diplomático español Camilo Villarino, conselleiro para Asuntos Transatlánticos e de Seguridade e Defensa na Embaixada de España en Washington. Nunha serie de correos electrónicos confidenciais coa axencia de intelixencia global Stratfor —aos que tivo acceso GC a través da base de datos de WikiLeaks—, Villarino non ocultou que a guerra en Libia ía proporcionar moitos réditos a países europeos como España pero, sobre todo, a Francia, Italia e Reino Unido.

Villarino mantivo durante marzo e abril de 2011 unha serie de correspondencias electrónicas con Marko Papic, analista xeopolítico de Stratfor. Nestas, e interpelado por Papic para coñecer mellor a posición de España respecto do conflicto en Libia, Villarino confesaba que a intervención europea respondeu a intereses comerciais e xeoestratéxicos, e no caso de España, tamén a súa submisión a Estados Unidos e o seu prestixio internacional.

Esta é parte do primeiro correo que Papic enviou o 21 de marzo de 2011 a Villarino, no que amosa o desconcerto que lle producía a ambigüidade de España:



Zapatero e Gadafi, en novembro de 2010 en Trípoli (Libia), durante o III Cumio UE-África | Fonte: *Moncloa*

> "Creo que Madrid se mantivo relativamente silencioso no período previo á intervención. Isto é algo que me estraña tendo en conta que España ten probábelmente o segundo maior interese en Libia despois de Italia. Repsol conta cunha gran cantidade de activos de enerxía e unha produción considerábel no país".
>
> Agora, polo que teño entendido, a forza aérea española moveu xa algúns dos seus efectivos a Sigonella [a base aérea da OTAN en Sicilia] e que tamén ofreceu dúas bases aéreas aos aliados. Porén, dáme a sensación de que Madrid non foi tan franco como os demás países europeos implicados.
>
> Podería aclararme o pensamento que hai en España neste momento? Gustaríame escribir unha serie de análises dos principais actores europeos nesta situación e España é, sen dúbida, un destes, mais é difícil evaluar o que Madrid pensa realmente".

Ese mesmo día, Carlos Villarino contestaba a Papic:

> "Vou tentar responder a súa primeira pregunta sobre a posición española. Creo que vostede ten razón, que nós non fomos tan francos como os demais, aínda que o Goberno (o presidente, o Ministerio de Asuntos Exteriores e o ministro de Defensa xa falaran con claridade hai días a prol dunha acción militar internacional, sempre e cando fose apoiada pola ONU e a Liga Árabe, coa fin de deter as violacións de dereitos humanos). Para entender mellor a posición de Madrid hai que diferenciar entre os intereses do Goberno en política exterior e en política doméstica.

> No referente á política exterior, España quere amosar a súa solidariedade cos Estados Unidos e as outras principais potencias europeas (coa excepción de Alemaña, moi influída pola situación interna e Westerwelle [ministro de Exteriores e vicecanceler]), así como demostrar que malia as súas extremas circunstancias económicas, España todavía pode ser un xogador na arena internacional.
>
> No que se refiere á política interna española, o Goberno atópase nunha posición difícil: haberá eleccións locais e autonómicas moi importantes o 22 de maio. As enquisas predicen grandes perdas a nivel nacional para o Partido Socialista, no poder. Unha parte do electorado socialista vai optar pola abstención e outra parte está disposta a votar a Izquierda Unida (coalición do antigo Partido Comunista e outros partidos de esquerda). As guerras -calquera guerra- non son moi populares entre a parte esquerda do Partido Socialista, onde aínda existe un importante grao de anti-americanismo, apoios ás políticas de Castro e Chavez, etc.
>
> Todo isto explica en parte a percepción que vostede e outros teñen de que España está apoiando a operación militar contra Gadafi (enviamos seis avións e estamos despregando unha fragata co sistema Aegis e un submarino), mais ao mesmo tempo non semella estar completamente detrás deste asunto. E certamente non se alardea disto.
>
> Ademais disto, o actual presidente do Goberno español [naquel momento, José Luis Rodríguez Zapatero] ten, por razóns biográficas persoais unha aversión natural contra o uso da forza (o seu avó, que era un oficial militar que se opuxo a Franco, foi executado sen xuízo durante a Guerra Civil española e viviu con ese recordo en casa dende que era un neno; seino por unha fonte directa) e quere diferenciarse do presidente Aznar e do seu apoio á guerra de 2003 en Iraq".

Tras estas primeiras consideracións, o diplomático español métese de cheo en materia e recoñece a existencia de intereses económicos, políticos e xeoestratéxicos nesta guerra:

> "É certo que temos intereses económicos en Libia (Repsol e outros), pero non está de todo claro se esta intervención vai ser ou non mellor, para ser honesto. Dependerá en gran medida de como evolucione a situación en Libia e no resto da rexión árabe. As últimas declaracións da Liga Árabe amosan moi ben a complexidade da situación e a cantidade de intereses que se cruzan (económicos, políticos e xeoestratéxicos)".

Ademais, Villarino móstrase moi crítico coa operación militar en Libia, que considera "un erro", e critica que non se puxesen en marcha previamente accións diplomáticas para iniciar un "diálogo político" co goberno de Gadafi, o que levou, na súa consideración, a "abrir a caixa de Pandora" da intervención militar empurrados, principalmente, polos "intereses de Sarkozy", presidente de Francia daquela:

> "No que se refiere á intervención militar, témome que reaccionamos tarde, cando o uso da forza militar era a única ferramenta dispoñíbel para nós e que sempre é un erro. Teriamos que ter intervido antes, non só con sancións, senón tamén cun diálogo político directo ao máis alto nivel posíbel co réxime de Gadafi: transformación mellor que revolución e mellor que guerra. Creo que non se explorou esa forma suficientemente e agora temos que abrir a caixa de Pandora dunha intervención (en gran medida propiciado por Sarkozy, polos seus propios intereses), que pode levarnos a lugares descoñecidos. A guerra é un asunto demasiado serio como para xogar con el para servir a propósitos electorais, anque me temo que xa debería estar acostumado a isto".

Os negocios das armas e a enerxía

Na seguinte táboa elaborada por Stratfor amósanse os países máis dependentes do petróleo libio.

IMPORT DEPENDENCE ON LIBYAN OIL

IMPORTERS	IMPORTS FROM LIBYA (BPD, 2010)	% OF LIBYA'S OIL EXPORTS	% OF TOTAL LOCAL CONSUMPTION
Italy	365,742	29%	24%
France	177,797	14%	10%
China	160,676	13%	2%
Germany	138,067	11%	6%
Spain	129,227	10%	9%
USA	60,553	5%	<1%
United Kingdom	50,815	4%	3%
Austria	32,867	3%	12%
Portugal	28,840	2%	11%
Netherlands	26,426	2%	2%
Ireland	21,814	2%	13%
Switzerland	21,576	2%	8%
Serbia	6,801	1%	8%

Sources: EIA and ITC Trademap

Poucos días despois, o 30 de marzo, Papic enviaba por email a Villarino o texto no que a axencia estadounidense Stratfor analizaba a intervención militar en Libia co título 'Special Series: Europe's Libya Intervention". Un documento de 19 páxinas no que se examinan os motivos da intervención europea e, en concreto, as posicións presentadas polo Reino Unido, Francia, Italia, Alemaña, Rusia e España.

Neste informe, os analistas salientaban que "os europeos non están unidos nas súas percepcóns dos obxectivos da operación, ou sobre como acometer a operación".

O informe é especialmente duro con Francia, "o país máis comprometido coa intervención en Libia" e cuxa ministra de Asuntos Exteriores, Michele Alliot-Marie, tivo que dimitir o 27 de febreiro de 2011 por ter aceptado unhas vacacións pagadas por un empresario tunesino próximo ao entón presidente Zine El Abidine Ben Ali, derrocado trala revolución popular e fuxido a Arabia Saudí. Stratfor lembra que Alliot-Marie mesmo chegou a ofrece ao ditador tunesino os servizos das forzas de seguridade francesas "para reprimir a rebelión".

Para os analistas, "o caso francés evidencia as relacións comerciais estreitas, os intereses enerxéticos e, a miúdo, as relacións persoais que os europeos tiñan cos líderes de Oriente Medio".

E Francia sería, para Stratfor, o mellor exemplo desa Europa sobre a que existe a percepción de que "non apoia adecuadamente as primeiras protestas pro-democráticas no mundo árabe", en gran parte porque "moitos gobernos europeos apoiaron activamente os rexímenes impugnados" polos cidadáns, destacan os analistas.

"De feito, os Estados da UE venderon a Gadafi 1,1 mil millóns de dólares en armas entre 2004, cando se levantou o embargo de armas, e 2011, e agardaban moito máis no futuro", lembran os expertos de Stratfor, que sinalan principalmente a Francia, Italia e Reino Unido como os países máis interesados nos negocios con Libia: "París e Roma, que traballaron duro para poñer fin ao embargo, foron particularmente activos neste comercio. En data tan recente como 2010, Francia estaba en conversacións con Libia para a venda de 14 avións de combate Dassault Mirage e a modernización dalgúns dos avións de Trípoli. Roma, pola súa banda, estaba en medio da negociación de mil millóns de dólares dos acordos anteriores aos disturbios. Medios británicos, pola súa parte, acusaran ao goberno británico anterior de dobregarse a Gadafi pola liberación de Abdel Basset Ali al-Megrahi, un libio que participou no atentado do voo 103 da Pan Am [en 1988]. Segundo numerosos informes, o goberno laborista do Reino Unido liberou a Al-Megrahi para que a compañía enerxética británica BP recibira concesións favorábeis en Libia".

A segunda percepción sobre o conflito en Libia e nos países árabes é o que Stratfor chama "a narrativa agora establecida en Occidente de que as protestas en curso son realmente unha explosión de sentimento pro-democrático no sentido occidental". Así é como xurdiu unha "percepción pública en Europa de que había que poñer sobre aviso aos rexímenes árabes de que as medidas enérxicas graves non serían toleradas, xa que as protestas son o comezo dunha nova xeira de democracia na rexión", explícase no documento.

Estas dúas percepcións, a dunha Europa tradicionalmente permisiva cos gobernos árabes e a dun movemento global pro-democrático nestes países, crearon un contexto no que "a represión de Gadafi contra os manifestantes é simplemente inaceptábel para París e Londres, e inaceptábel para a opinión pública europea", saliéntase no informe.

Pero os analistas de Stratfor tamén cuestionaron a estratexia europea de introducir aos rebeldes do Este de Libia na narrativa dos movementos pro-democráticos árabes que tentan derrocar a rexímenes brutais, xa que non estaba "nada claro cales eran as súas intencións para unha Libia post-Gadafi".

Na seguinte infografía de Stratfor amósanse os intereses enerxéticos e armamentísticos de España, Francia, Reino Unido, Italia e Alemaña.

Na seguinte achega publicaremos o máis salientábel do documento de Stratfor sobre os papeis que xogaron España, Reino Unido, Francia, Italia, Alemaña e Rusia na guerra de Libia e publicaremos en GC PLUS (só para subscritores) dous documentos en formato pdf cos correos de Camilo Villarino e o informe completo da axencia de intelixencia estadounidense.

ANEXO XV: Publicación 7 de los correos de Stratfor.

Os intereses europeos na guerra en Libia

Segunda achega sobre os intereses dos países europeos no conflito libio na que analizamos polo miúdo as estratexias de España, Italia, Reino Unido, Francia e Rusia para obter beneficios comerciais, políticos e xeoestratéxicos. Documentos orixinais no interior da axencia Stratfor.

› Os negocios de España na guerra libia

Por Alberto Quian | Madrid | 14/01/2013 | Actualizada ás 08:00

Tras publicar os correos electrónicos que intercambiaron o analista xeopolítico de Stratfor Marko Papic e o diplomático español Camilo Villarino —conselleiro para Asuntos Transatlánticos e de Seguridade e Defensa na Embaixada de España en Washington— sobre os intereses españois na guerra en Libia, e logo de aproximarnos aos proveitos do conflito para España, Italia, Reino Unido, Francia e Alemaña, imos ver agora polo miúdo, país por país, cales foron os intereses que motivaron a súa participación na guerra en Libia, segundo o informe de Stratfor publicado en marzo de 2011.

Silvio Berlusconi e Muamar Gadhafi, no ano 2009 | Fonte: *daveeza en Flickr.com*

España

Para os analistas de Stratfor, logo da retirada das tropas de Iraq ordenada por Zapatero nada máis chegar ao poder no ano 2004, a decisión de intervir en Libia respondeu non só a "unha forma de revitalizar a imaxe de España como un país capaz ter unha presenza activa internacional cando sexa necesario, especialmente no Mediterráneo, a súa área de interés nacional", senón tamén a "un esforzo de última hora por elevar o perfil dun impopular goberno antes das eleccións a principios de 2012".

Os analistas de Stratfor falan dun país tradicionalmente "aillado política e xeograficamente" do núcleo de Europa e pouco preocupado polos "beneficios en seguridade que dá ser membro da OTAN".

No informe se destaca que as maiores preocupacións internacionais de España están relacionadas coa "súa proximidade co Norte de África e os conseguintes efectos negativos da delincuencia organizada e o contrabando". Ademais, apúntase que "as garantías de seguridade da OTAN non se aplican aos enclaves españois de Ceuta e Melilla" e consideran que "se podería argumentar que a pertenza á OTAN de España sen dúbida sería unha razón psicolóxica para que Marrocos reconsidere os seus plans de apoderarse dos dous territorios".

Informe da axencia de intelixencia Stratfor sobre os intereses europeos na guerra en Libia

Os expertos de Stratfor observan que a intervención de España na guerra en Libia pretendía "ilustrar a súa solidariedade cos Estados Unidos e as outras potencias europeas". E para Rodríguez Zapatero, en particular, "era unha forma de ilustrar que Madrid non ten medo da acción militar internacional" e de demostrar que, "malia a crise económica considerábel e os temores de que España podería ser a próxima economía da eurozona, despois de Portugal, que tería que ser rescatada", España aínda podía "desempeñar un papel importante na política internacional".

Pero non convíña facer moito ruído para non axitar aos sectores máis esquerdistas do socialismo español, tradicionalmente opostos a calquera intervención militar. Así, Stratfor explica como o Goberno socialista estaba tratando de elevar o perfil internacional de España do xeito máis silencioso posíbel, "sen moita xactancia na casa para evitar unha maior erosión do apoio das súas bases", dise no documento.

Ademais dos intereses políticos, existían tamén intereses estratéxicos e comerciais en Libia, se ben "non tan grandes como os de Italia", aclara o informe.

Stratfor sinala como exemplo a enerxética española Repsol, que extraía en Libia un 8,3 por cento da súa produción global no ano 2009. Para os analistas, "non se trata dunha cantidade insignificante e é comparábel ao 10,7 por cento que o xigante enerxético italiano ENI extraía neste país".

As importacións españolas de petróleo de Libia era comparábeis ás de Francia, representando o 9 por cento do consumo total do país, pero estaban lonxe do 25 por cento do total de petróleo que consume Italia.

O informe tamén destaca que se ben a empresa francesa Total extraía máis petróleo de Libia que Repsol, como empresa máis grande que a española, o ouro negro de Libia representaba unha menor proporción do total da compañía francesa. "Neste sentido, Repsol non estaba necesariamente instisfeita co *status quo* de Gadafi en Libia" e Stratfor vía "probábel" que a compañía "mirase con receo os movementos franceses e británicos".

Por último, a axencia estadounidense apunta que España tiña que "ter en conta o que significa a inestabilidade de Libia na rexión", con Marrocos tan próximo ao contaxio das revolucións populares.

"Madrid non pode opoñerse á intervención internacional en Libia, xa que non quere sentar un precedente que pode supoñer un revés en breve. Un cambio de réxime en Marrocos, por exemplo, podería colocar os enclaves norteafricanos de Madrid nunha situación insostíbel, ou podería producir un éxodo de migrantes que España tería que contrarrestar coa intervención agresiva da forza naval, do mesmo xeito que Italia ameaza con comezar a facelo cos inmigrantes chegados de Tunes e Libia. Dito isto, Marrocos non se achega ao punto de inestabilidade libio ou mesmo aos disturbios de Tunes e Exipto", arguméntase.

O informe sentencia que o interés de España en participar no conflito respondeu á necesidade de "ter voz e voto na resolución posterior á intervención" e non deixar que Francia e Reino Unido tomasen vantaxe comercial "usando o seu apoio aos rebeldes libios para mellorar as súas posicións", coméntase no documento, no que se insiste na idea de que o Goberno español "non se fiaba" das estratexias francesa e británica, o que levou a España a posicionarse xunto a Alemaña e Italia a prol da opción do exilio de Gadafi para facilitar a fin da intervención.

Francia

Francia xa tiña en Trípoli a un exportador importante de enerxía e a un gran cliente de armas. Mais segundo Stratfor, a intervención de Francia tamén tivo que ver coas políticas intra-europeas.

O país galo foi o defensor más vociferante da intervención en Libia e da lexitimidade dos rebeldes de Benghazi. Para os analistas, os intereses franceses nesta guerra dividíanse basicamente en dúas categorías: a política nacional e as relacións intra-europeas.

Por un lado, o goberno de Sarkozy evitara nun primeiro momento o recoñecemento dos movementos pro-democráticos que se estaban dando nos países árabes e mesmo chegara a ofrecer axuda ao Goberno tunesino para facer fronte aos manifestantes. Ademais, Francia tiña unha bomba de reloxería no seu propio territorio, cunha masiva poboación musulmana asentada no país. Para Stratfor, a reacción anti-Gadafi de Francia foi "máis ca unha excesiva compensación" polo posicionamento inicial do goberno de Sarkozy a prol dos rexímenes instaurados no Norte de África. Había en xogo, segundo os expertos, algo máis que a imaxe do país galo. A Sarkozy preocupábanlle moito as eleccións presidenciais de 2012 e o papel de Francia como potencia militar europea, co que podería contrarrestar ante a opinión pública francesa o omnímodo poder que vén gañando Alemaña coa crise da débeda soberana na zona euro.

"A intervención en Libia é un xeito de reafirmar ante Europa, pero sobre todo ante Alemaña, que Francia segue á cabeza do continente en asuntos exteriores e militares. É unha mensaxe que di que se Europa quere ser tomada en serio como unha potencia mundial, necesitará o poder militar francés", argúen os informantes de Stratfor, que apuntan ademais á alianza militar nuclear entre París e Londres, formalizada o 2 de novembro de 2010, para "contrarrestar o esmagador poder económico e político de Alemaña na Unión Europea".

O informe tamén sinala as potenciais melloras comerciais para Francia coa guerra en Libia. "A principal compañía francesa de enerxía solar, Total SA, está implicada en Libia, pero non na mesma medida que a italiana ENI ou a alemá Wintershall. Tendo en conta as abondantes reservas enerxéticas de Libia, e en gran parte inexploradas, as empresas francesas de enerxía poderían sacar proveito da axuda aos rebeldes para que tomen o poder en Trípoli", advertíase no documento.

Ademais, Francia viña facendo grandes negocios con Libia coa venda de armamento. Entre o ano 2004 —cando a Unión Europea levantou o embargo de armas ao país norteafricano— e 2011, Trípoli comprou armas a Francia por uns 500 millóns de dólares, máis que a calqueroutro país de Europa. Porén, o Goberno italiano estaba en negociacións para vender ao Goberno de Gadafi armamento por máis de mil millóns de dólares, relegando a Francia no papel de principal subministrador armamentístico de Libia.

Reino Unido

Para o Reino Unido, Libia ofrecía unha "promesa de explotación enerxética" e o derrocamento de Muamar Gadafi faría posíbel desenvolver fortes relacións comerciais que antes non existían, clarifican os expertos de Stratfor.

No caso británico, a principal motivación para intervir en Libia foron os intereses enerxéticos. O xigante enerxético BP non tiña produción en Libia, anque asinara en 2007 un acordo con Trípoli para perforar pozos en terra e alta mar a cambio de mil millóns de dólares. Estas negociacións só chegaron a bo porto cando o Goberno escocés decidiu liberar ao terrorista de Lockerbie Abdel Baset al-Megrahi por "razóns humanitarias", en agosto de 2009, recordan os analistas. "Agardábase que morrese de cancro de próstata aos poucos meses de ser liberado, pero se supón que segue vivo en Trípoli", especúlabase con razón no informe, pois Al-Megrahi finou o 20 de maio de 2012 na capital de Libia a causa dun cancro.

O informe lembra que o Goberno laborista foi daquela obxecto de fortes críticas pola liberación de Al-Megrahi. "Os medios británicos especularon, non de todo inxustamente, con que a decisión representou un esforzo para poñer en marcha a produción de BP en Libia e suavizar así as relacións entre Londres e Trípoli. BP anunciou en 2009 que tiña previsto investir 20.000 millóns de dólares na produción de petróleo de Libia nos próximos vinte anos", aclárase no documento.

Ademais, a catástrofe ecolóxica provocada por BP no Golfo de México o 20 de abril de 2010 urxiu a BP e o Goberno británico a acelerar a súa estratexia para Libia. "O desastre de BP causoulle 17,7 mil millóns de dólares en perdas en 2010 e a compañía tivo que crear un fondo de compensación de 20 mil millóns máis. As estimacións dos custos potenciais adicionais do derrame oscilan entre os 38.000 e os 60.000 millóns de dólares, creando un futuro incerto para BP en Estados Unidos. O desastre tamén permitiu que os competidores de BP se queixasen das súas posíbeis operacións en alta mar nun futuro, algo que o ministro de Asuntos Exteriores italiano, Franco Frattini, salientou argumentando que até que se completase a investigación sobre o desastre do pozo Macondo, BP debería absterse de perforacións en Libia mar adentro, no Mediterráneo. A queixa era moi probábelmente un intento por parte de ENI de complicar as operacións de BP en Libia, cuestionando o seu historial ambiental en América do Norte", relátase no informe da axencia estadounidense.

Así as cousas, Stratfor considerou que "Londres podería obter o máximo proveito coa destitución de Gadafi ou gañándose a lealdade dun goberno controlado polos rebeldes nunha especie de semi-Estado independente no Este de Libia. Sen produción de petróleo en Libia e a diminución da venda de armas dos franceses e italianos nunha cantidade considerábel, o Reino Unido podería beneficiarse substancialmente dun novo liderazgo en Trípoli ou mesmo en Benghazi", conclúe o documento.

Italia

Os custos dunha guerra contra Gadafi non ían ser os mesmos para todos os países europeos participantes. Especialmente importantes ían ser para Italia, que, segundo Stratfor, tiña máis que perder se Gadafi conservase o poder". E este erá "o maior problema para a unidade europea", destaca Stratfor.

O caso italiano é singular. Como se recorda no informe de Stratfor, os avións das forzas armadas daquel país interviron en Libia sen executar un só disparo. Isto "non foi casual", segundo os analistas, xa que "foi parte da estratexia de prevención de Roma" como tradicional aliado de Gadafi.

Segundo as fontes italianas de Stratfor, este país era o que "máis tiña que perder" entre os aliados europeos, xa que "os seus intereses comerciais, enerxéticos e de seguridade nacional" serían "directamente impactados polo destino de Libia". Por esta razón, nos primeiros momentos Italia posicionouse do lado de Gadafi, expresando a súa preocupación pola autoproclamación do Emirato Islámico de Benghazi o 21 de febreiro de 2011, facéndose eco dunha declaración do fillo de Gadafi, Seif al-Islam.

Mais ao final Italia non puido máis que sumarse á coalición occidental como membro da OTAN e da UE, prestando sete bases aéreas e avións para a intervención militar. Con todo, "Italia abstívose de xogar un papel agresivo contra Gadafi" seguindo unha "estratexia destinada a permitirlle manter un equilibrio cos rebeldes do Este e con Gadafi no Oeste do país. Roma simplemente ten demasiados intereses en Libia como para decantarse por un lado e aferrarse a ese", argumentáse no documento de Stratfor.

Ademais, Italia temía que no momento no que Estados Unidos deixase vía libre a Francia e Reino Unido á fronte da operación militar, "os seus intereses enerxéticos e de seguridade nacional poderían quedar a mercé dos países que procuraban tomar a dianteira nunha Libia post-Gadafi", prosegue o informe. No documento saliéntase a desconfianza de Roma respecto as intencións de París e Londres de expandir os seus intereses enerxéticos e de negocios, grazas ao agradecemento que agardaban dos rebeldes unha vez consumado o cambio de réxime en Libia, ou polo menos na parte oriental do país. Como ben lembran os analistas de Stratfor, os propios líderes rebeldes insistiron en que os vínculos económicos serían calibrados de novo para "reflexar o apoio que os distintos países europeos ofreceron ao levantamento".

A tradicional alianza de Italia e Libia vén de lonxe. Stratfor lembra, por exemplo, que a enerxética ENI comezou a operar nom país africano en 1959 e que nunca saíu deste, nin sequera cando o resto de Occidente rexeitou, cando menos en apariencia, a Gadafi na década de 1980 debido a súa asociación co terrorismo. "Este compromiso con Libia permitiulle a Roma un negocio enerxético moi lucrativo e contratos de armas, unha vez que Gadafi renunciou ao terrorismo en 2003. Libia representaba no ano 2009 arredor do 15 por cento do total da produción de hidrocarburos de ENI, a produción de 108.000 barrís de petróleo por día e a produción de 8,1 millóns de metros cúbicos de gas natural, enumérase no documento da axencia de intelixencia, no que se sinalan os riscos que corría Italia de aumentar a súa dependencia do gas natural ruso no caso de que a crise libia se prolongase no tempo.

Ademais, Italia foi un dos principais provedores de armas de Gadafi dende que se levantara o embargo a Libia en 2004, "un paso para o que presionou fortemente Italia", dise no informe, no que se salienta que Italia tiña asinados contratos co país africano dende 2004 de preto de 500 millóns de dólares, unha cantidade algo inferior ao valor das entregas militares francesas. E estaba en proceso de negociación duns 1,05 mil millóns de dólares en contratos militares antes de que comezasen os disturbios en Libia. Os acordos incluían un gran sistema de control e seguridade fronteirizo contratado ao grupo industrial Finmeccanica por 300 millóns de dólares e a construción de buques por valor de 600 millóns encargados a Intermarine Spa.

Stratfor tamén destaca que "o fluxo de capital e investimentos non era unilateral", xa que "o fondo soberano de Libia investiu en empresas financeiras e industriais italianas". Segundo os datos aportados pola axencia, "o Fondo soberano de investimento de Libia posuía arredor do 1 por cento de ENI e manifestara a súa intención de aumentar a súa participación até o 10 por cento; o 7,2 por cento de UniCredit, o maior banco de Italia, e o 2 por cento do fabricante de armas Finmeccanica".

Por último, Libia tamén plantexaba unha cuestión de seguridade nacional para Italia polo gran número de emigrantes *ilegais* chegados dende o país norteafricano. Un problema para Italia que ambos os dous países tentaron resolver mediante a sinatura dun tratado de amizade polo que Libia detería o fluxo de emigrantes a cambio de investimentos no país.

Alemaña

A decisión do Goberno alemán de non intervir en Libia "non foi meramente un esforzo para compracer as sensibilidades históricas do país xermano" e máis antes dunhas eleccións tan importantes como as que se ían celebrar no Estado de Baden-Württenberg. Para os analistas de Stratfor existían outros dous factores estratéxicos: en primeiro lugar, o feito de que "Reino Unido, Francia e Italia tiñan intereses enerxéticos en Libia e querían máis, o cal non quere dicir que Alemaña non os tivese, xa que a compañía enerxética Wintershall estaba especialmente implicada, pero eses intereses non eran tan críticos para o país"; en segundo lugar, o feito de que os franceses consideran o Mediterráneo a súa área de influencia e xa mantiveran importantes desacordos con Alemaña sobre a Unión para o Mediterráneo.

Para Stratfor, o fondo da non intervención alemá é o seguinte: "A disposición de enfrentarse a todos os seus aliados atlánticos debido á política interna e a falla de interese nacional representa unha forma de autoafirmación: Alemaña está amosando a súa vontade de poñer a súa política interna por enriba dos seus compromisos cos seus aliados".

Os analistas de Stratfor consideran que, do mesmo xeito que fixo en Afganistán, "Berlín podería ter optado por enviar unha forza simbólica dun puñado de combatentes para facer cumprir a zona de exclusión aérea, ao igual que Noruega, Dinamarca, Bélxica ou Holanda". Pero os expertos sospeitaron que "Berlín decidiu opoñerse a Francia e minar calquera das motivacións principais de París para a intervención, é dicir, para demostrar que Europa sen unha Francia militarizada está á altura da condición de gran potencia".

Rusia

Para Stratfor, "a abstención de Rusia foi un movemento calculado deseñado para facilitar a intervención en Libia". Como membro permanente do Consello de Seguridade das Nacións Unidas, o veto de Rusia tería torpedeado a intervención, pero segundo os analistas, Rusia tiña "intereses en que Occidente, e en particular Estados Unidos, participasen nun novo conflito en Medio Oriente".

Os motivos son obvios: as inestabilidades na zona fan aumentar o prezo dos barrís de petróleo e beneficia as exportacións do ouro negro ruso. E en particular, a guerra en Libia beneficiaba as exportacións a Europa do petróleo e do gas natural de Rusia, que podería gañar mercados como o italiano, máis dependente dos recursos enerxéticos libios.

Os especialistas de Stratfor observan tamén un especial interese de Rusia en manter a Estados Unidos ocupado en conflitos en Oriente Medio para que non desvíe a súa atención e maquinaria económica cara a zona de influencia de Rusia: Europa Central e Oriental, Asia Central e o Cáucaso.

E en terceiro lugar, a situación en Libia daba aos dirixentes rusos "outra oportunidade para criticar publicamente a Estados Unidos", xa que "cando Putin fixo as declaracións comparando a intervención en Libia cunha cruzada, fíxoo nunha fábrica de mísiles balísticos o mesmo día en que o secretario de Defensa de Estados Unidos, Robert Gates, estaba en San Petersburgo reunido co presidente Dmitri Medvedev para falar da defensa antimísiles". Para os analistas xeopolíticos, "a elección das palabras de Putin e o lugar nas que as dixo foron simbólicos, levando a mensaxe de que Estados Unidos ten obxectivos expansionistas e militaristas contra Rusia, obxectivos polos que Rusia xustifica a adopción de medidas en contra".

"A intervención en Libia ofrece a Moscova unha nova oportunidade para criticar a Estados Unidos como unha potencia agresiva e dálle outra vía a través da cal expresar o seu desacordo permanente con Washington", conclúe o informe da axencia de intelixencia.

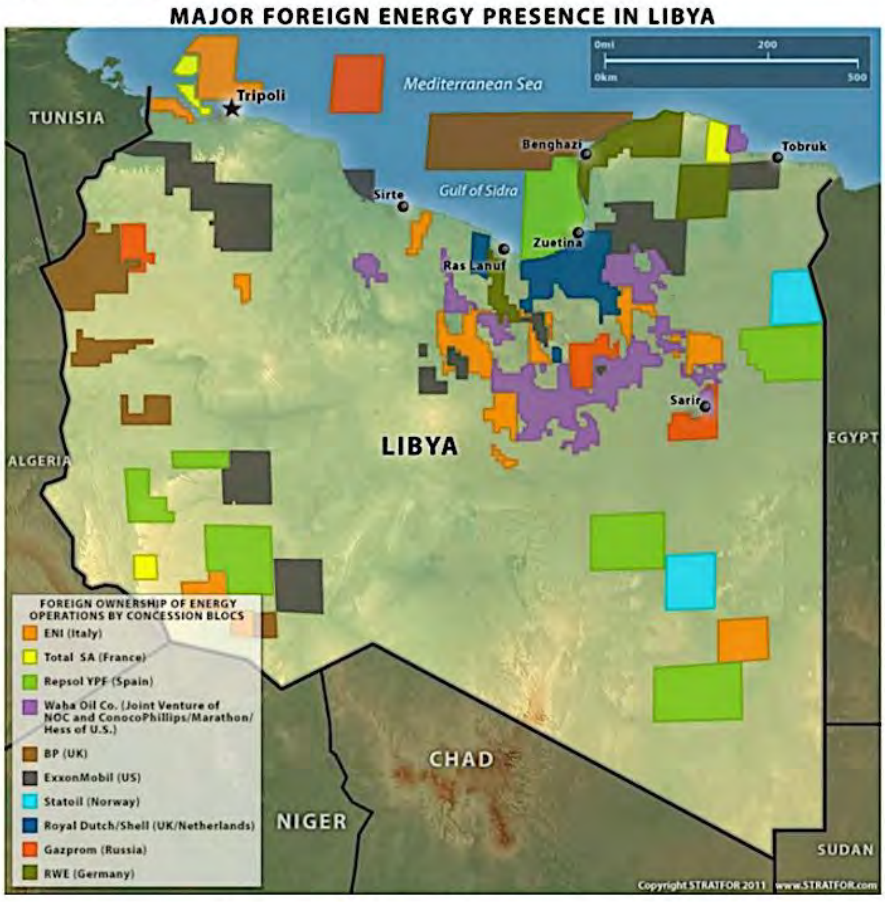
Países máis dependentes do petróleo libio

IMPORT DEPENDENCE ON LIBYAN OIL

IMPORTERS	IMPORTS FROM LIBYA (BPD, 2010)	% OF LIBYA'S OIL EXPORTS	% OF TOTAL LOCAL CONSUMPTION
Italy	365,742	29%	24%
France	177,797	14%	10%
China	160,676	13%	2%
Germany	138,067	11%	6%
Spain	129,227	10%	9%
USA	60,553	5%	<1%
United Kingdom	50,815	4%	3%
Austria	32,867	3%	12%
Portugal	28,840	2%	11%
Netherlands	26,426	2%	2%
Ireland	21,814	2%	13%
Switzerland	21,576	2%	8%
Serbia	6,801	1%	8%

Sources: EIA and ITC Trademap Copyright STRATFOR 2011 www.STRATFOR.com

Mapa coas principais compañías enerxéticas estranxeiras en Libia



Intereses enerxéticos e armamentísticos de España, Francia, Reino Unido, Italia e Alemaña

Intereses enerxéticos e armamentísticos de España, Francia, Reino Unido, Italia e Alemaña

Descarga os correos electrónicos entre o diplomático español Camilo Villarino e Marko Papic, analista de Stratfor.

Descarga o informe de Stratfor 'Special Series: Europe's Libya Intervention'.

ANEXO XVI: Publicación 8 de los correos de Stratfor

Que pactou o PP cos mercados antes do 20N?

Un informe do fondo Emerging Sovereign Group di que o PP prometía aos inversores internacionais "recortes e reformas radicais" cando chegase ao poder e admite que Rajoy ocultou as súas intencións para non perder votos.

› A estratexia do PP en 2011: pactar recortes cos mercados e negalos ante a opinión pública

Por Alberto Quian | Madrid | 20/02/2013 | Actualizada ás 08:00

O PP argallou un dobre discurso nos meses previos ás eleccións xerais de 2011: un para compracer aos mercados e outro, antagónico, dirixido aos cidadáns para gañar apoio electoral. Así o recoñecía o fondo estadounidense Emerging Sovereign Group nun informe dirixido aos seus clientes en xullo de 2011 do que se desprende un posíbel engano do PP aos electores.

Aznar e Rajoy nun acto de FAES | Fonte: *pp.es*

Durante o ano 2011, os conservadores deseñaron e puxeron en práctica, desde a oposición ao Goberno de Zapatero, unha dobre estratexia que consistía, por un lado, en anunciar recortes e reformas radicais aos mercados en reunións secretas, e polo outro, tentar a través do seu aparato de propaganda política convencer á opinión pública española de que non habería reformas dramáticas nin recortes radicais ás clases medias e traballadoras se os *populares* gañaban nas urnas o 20 de novembro.

Enganaron, pois, os *populares* á cidadanía? Cometeron fraude electoral co engano? Que se falou e pactou nesas reunións privadas cos axentes dos mercados internacionais? Por que unha vez no Goberno o PP culpou ao PSOE de obrigarlle a aplicar recortes, subas de impostos e reformas que xa tiñan planeados previamente pero que negaron durante a precampaña e campaña electoral? Que sabía e que intencións tiña o PP nos meses previos aos comicios para mover fichas cos inversores internacionais nesas reunións?

A consigna dentro do PP durante a precampaña e campaña electoral en 2011 foi negar ante a opinión pública española calquera medida impopular que poidese restarlle votos. Todo pintaba bonito daquela no discurso dos *populares*: salvagarda da educación, sanidade e pensións, baixada de impostos, pulo ás contratacións indefinidas, non abaratar os despedimentos, axudas aos pequenos e medianos empresarios, salvar aos máis afectados polas hipotecas das gadoupas dos banqueiros... Á par que pactaba cos mercados os duros recortes que logo aplicaría no Goberno, o PP autodefiníase en mitins, entrevistas e roldas de prensa como "o partido dos traballadores" e anunciaba que o cambio que ía aplicar ía ser "o cambio da xente, do pobo, non o das grandes finanzas" (hoxe, nada máis lonxe da realidade).

Así foi o discurso do PP dirixido á cidadanía nos meses e semanas previos ás eleccións xerais, e nos primeiros días no Goberno:

> **Esperanza Aguirre, ex-presidenta da Comunidade de Madrid**: "A sanidade pública custa moitos cartos e a pagan as cotizacións á Seguridade Social; o copago non a fai sostíbel [...] En Madrid non haberá copago. Pagar 1€ por algo que vale 100 non ten sentido" (trala reunión do Comité rexional do PP de Madrid o 29 de marzo de 2011).
>
> **Esteban González Pons, vicesecretario xeral de Estudos e Programas do PP**: "Os banqueiros agora din que apoian ao Partido Popular... Pois benvidos sexan, porque son os últimos en chegar. A xente, os seus clientes, os que pagan as hipotecas, hai xa moito que apostaban polo Partido Popular. Primeiro, o 22 de maio [celebración de eleccións municipais en todo o Estado e autonómicas en 13 comunidades] tivemos que ver como o pobo apoiaba ao Partido Popular mentres os banqueiros apoiaban a Zapatero, para que agora os banqueiros digan que tamén apoian ao Partido Popular. Estan tentando apuntarse ao cabalo do cambio, pero lembrolles desde esta tribuna, que é a do PP, que o cabalo do cambio é o da xente, é do pobo, non é o cabalo das grandes finanzas. Faremos economía, pero para crear emprego, non para que os banqueiros gañen máis" (rolda de prensa posterior á reunión do comité de campaña do PP o 1 de agosto de 2011).
>
> **María Dolores de Cospedal, secretaria xeral do PP**: "Nunca se saíu en España, nunca, nunca, dunha crise económica subindo os impostos; nunca" (programa de Ana Rosa en Telecinco o 6 de setembro de 2011).
>
> **Mariano Rajoy, presidente do Goberno**: "Non estou de acordo con que o contrato temporal en España se converta na norma xeral e o indefinido na excepción. Eu quero que o indefinido sexa a normal xeral e o temporal a excepción" (Foro de Emprego do PP en Las Palmas, 10 de setembro de 2011).
>
> **Esteban González Pons, vicesecretario xeral de Estudos e Programas do PP**: "O PSOE quere subir os impostos para que todo siga como está; o Partido Popular quere baixar os impostos para que todo cambie" (durante o comité de dirección do PP o 3 de outubro de 2011).
>
> **Cristóbal Montoro, ministro de Facenda**: "Facer reformas non significa sacrificios para aqueles cidadáns que non teñen que soportar máis sacrificios, que xa pagaron moi duramente esta crise" (Ponencia 'Estabilidade e reformas para o emprego' na convención nacional do PP en Málaga o 6 de outubro de 2011).
>
> **Esteban González Pons, vicesecretario xeral de Estudos e Programas do PP**: "Nós non somos partidarios de abaratar o despedimento, somos partidarios de abaratar a contratación. Nun mercado laboral que está perdendo traballadores, no que se está despindo a traballadores, só falta que aos empresarios se lles facilite o despedmento. O que hai que facer é facilitar a contratación, abaratar a contratación para que máis traballadores entren a traballar, e reducir o número de contratos para que todos tendan a ser fixos (...) O Partido Popular non vai apoiarr abaratar o despedimento en ningún caso; vai apoiar abaratar a contratación en todos os casos. (...) Non se poder facer unha reforma laboral sen contar cos sindicatos. Haberá que falar Goberno, patronal e sindicatos" (declaracións no espazo 'Los Desayunos de TVE' o 20 de outubro de 2011).

> **Mariano Rajoy, presidente do Goberno**: "Voulle meter a tesoira a todo, agás as pensións públicas e, anque sexan competencia das comunidades autónomas, a sanidade e a educación, onde non quero recortar os dereitos dos cidadáns" (declaracións en ABC Punto Radio o 4 de novembro de 2011).
>
> **Mariano Rajoy, presidente do Goberno**: "Eu teño que dicir que a miña intención é non subir os impostos, porque creo que nun momento como este, e máis aos pequenos e medianos empresarios, ou ás empresas, coas dificultades que están pasando, non me parece o máis razoábel" (debate de investidura o 19 de decembro de 2011).

> **Soraya Sáenz de Santamaría, vicepresidenta do Goberno**: "Este Goberno vese obrigado a unha suba temporal de determinados impostos" (rolda de prensa posterior ao consello de ministros do 30 de decembro de 2011).

> **Luis de Guindos, ministro de Economía**: "Mañá aprobamos a reforma laboral e veredes que vai ser moi agresiva (...). Xa verás, xa verás" (conversa co vicepresidente económico da Unión Europea, Olli Rehn, o 9 de febreiro de 2012).

O tempo demostrou que nada do que prometeron os conservadores se cumpriu. A estratexia do PP para xustificar os recortes e reformas foi a de costume: culpar ao PSOE de ter deixado España patas arriba e de ocultar as contas reais do Estado. Mais se os *populares* non coñecían o alcance real da crise e estaban convencendo aos cidadáns de que se podía baixar os impostos e non aplicar recortes aos traballadores nin reformas dramáticas na sanidade e a educación, é obrigado preguntar por que antes das eleccións xerais estaban prometendo aos inversores "recortes orzamentarios e reformas radicais"? E en que termos o fixeron?

Este é o parágrafo do informe de Emerging Sovereign Group do 31 de xullo de 2011:

> "A estratexia do PP para gañar a confianza dos mercados parece ser que é dispoñer do ex-presidente Aznar e contarlle aos inversores internacionais en reunións privadas que un goberno do PP rapidamente faría recortes orzamentarios e reformas radicais. Ao mesmo tempo, Rajoy minimiza na prensa doméstica a posibilidade de tales medidas drásticas, xa que obviamente isto non lle permitiría gañar votos".

Este pequeno pero revelador parágrafo evidenciaría que o actual Goberno e o Partido Popular mentiron aos cidadáns durante os meses e semanas previos ás eleccións. Rajoy, Aznar e todo o aparato económico do PP terían argallado e pactado cos mercados, antes das eleccións xerais, os durísimos recortes e reformas que vén aplicando o Goberno conservador. Unhas medidas que ocultaron aos cidadáns a conciencia, polo que se desprende do informe de Emerging Sovereign Group.

Baste repetir que o 9 de febreiro de 2012, De Guindos rendía contas ante o vicepresidente económico da Unión Europea, Olli Rehn, anunciándolle o cumprimento de parte dos "recortes e reformas radicais" pactados: "Mañá aprobamos a reforma laboral e veredes que vai ser moi agresiva".

Encomenda dos mercados ao PP?

A esperanza dos mercados estaba xa depositada no PP. Do informe de Emerging Sovereign Group pode deducirse que as reunións dos inversores cos *populares* estiveron destinadas a marcar novas políticas encamiñadas a satisfacer aos mercados, a custa do benestar dos cidadáns, con recortes e reformas radicais. A perda de confianza dos mercados no Goberno socialista tería precipitado as negociacións dos inversores internacionais co PP, partido no que mantiñan a esperanza de que aplicaría as medidas que esixían os mercados a España. Así, Emerging Sovereign Group explicaba no documento: "O Goberno actual perdeu por completo a confianza dos mercados tras desperdiciar máis dun ano desde o inicio da crise no que se levaron a cabo poucas reformas reais e, no canto, tentaron esaxerar unha moi débil reforma das pensións e unha reforma do mercado laboral inexistente. A esperanza é que a perspecvtiva dun novo Goberno o 1 de xaneiro de 2012 estabilizará os mercados".

Porén, daquela o fondo estadounidense tiña serias dúbidas sobre as posibilidades reais de vitoria para Rajoy nas eleccións do 20-N. Emerging Sovereign Group apostaba pola política financeira "conservadora" do PP, mais consideraba a Rajoy un candidato "moi débil".

"A fiestra da resposta política está pechada"

Os analistas de Emerging Sovereign Group recoñecían no seu informe ser "máis pesimistas que o mercado" sobre a situación da economía española, se ben advertían de que existía a posibilidade de "evitar o rescate" se se implementaban "de xeito rápido" as "medidas políticas radicais necesarias".

A desconfianza do fondo neoiorquino traducíase no seu convencemento de que España estaba "paralizada" politicamente, que xa lle pasara o tempo das decisións políticas e que era hora de que os mercados tomasen as rendas da situación. "A fiestra da resposta política está cerca de pecharse ou pode que xa o estea", sentenciaban os analistas.

Un dos factores que, segundo o fondo estadounidense, xogaba contra os intereses de España era o fluxo de "noticias domésticas negativas" que contribuían a "un debilitamento da economía" e a unha nova "recesión", xunto co "aumento da parálise política que se traduciu no anuncio o 29 de xullo de eleccións anticipadas para ser celebradas o 20 de novembro", o "deterioro das finanzas das autonomías", a "lentitude da reforma do sector financeiro (especialmente a recapitalización das caixas)" e o "contaxio de Grecia", coméntase no documento.

O "problema" autonómico

Cabe salientar que para estes analistas os problemas das finanzas autonómicas estaban sendo cruciais no estado comatoso da economía estatal. "O problema", explicaban, "é que é practicamente imposíbel determinar o alcance total do problema das finanzas autonómicas dada a falla de transparencia e o retraso no subministro de datos. De feito, contáronnos ex-funcionarios de alto nivel do Ministerio de Economía que non hai auditorías independentes das finanzas públicas autonómicas e que as últimas auditorías non independentes se realizaron no ano 2008 nalgúns casos e no 2005 noutros".

GC conseguiu o documento de Emerging Sovereign Group grazas ao acceso que WikiLeaks deu a este xornal á base de datos cos correos da axencia de intelixencia global Stratfor.

Descarga en GC Plus o documento do fondo Emerging Soverign Group.

ANEXO XVII: Publicación 9 de los correos de Stratfor.

Pemex (I): corrupción, crimes e inseguridade no novo dono de Barreras

GC inicia a publicación dunha serie de artigos de análise sobre Petróleos Mexicanos (Pemex), a empresa paraestatal que se fará co control do estaleiro vigués Hijos de J. Barreras, a maior factoría naval privada de Galicia. Os correos da axencia Stratfor desvelados por WikiLeaks mostran as eivas do novo actor clave do naval galego.

- Os investimentos de Pémex
- A prensa mexicana dá por feito que Pemex construirá en Galicia

Por Alberto Quian | Vigo | 09/05/2013 | Actualizada ás 08:00

A historia máis recente de Petróleos Mexicanos (Pemex) non convida a unha lectura positiva e optimista para o futuro do naval galego coa súa incursión no estaleiro vigués Hijos de J. Barreras. Na última década, a empresa pública paraestatal mexicana estivo zarrapicada por casos de corrupción, neglixencias, narcotráfico, secuestros, roubos, inseguridade, accidentes laborais, problemas financeiros, investimentos e alianzas fallidos, subdesenvolvemento tecnolóxico, sindicalismo oportunista...

Estación de servizo de Pemex | Fonte: *Coolcaesar*

A recente visita a México do presidente da Xunta de Galicia, Alberto Núñez Feijóo, foi determinante para vender o 51% da maior factoría naval privada de Galicia ao Estado mexicano, propietario de Pemex. Caprichos ou broma do destino, casualidades ou coincidencias, o certo é que Feijóo chegou ao país azteca coa sombra do narcotráfico pesando sobre a súa carreira política, logo de saberse que mantivo unha estreita relación co traficante arousán Marcial Dorado. Alí, en México, o presidente aplanou o camiño para que tome as rendas de Barreras a paraestatal Pemex, unha empresa tamén con denuncias de corrupción e supostos contactos coas redes do narcotráfico e o crime organizado mexicano.

Problemas de seguridade

A historia recente de Pemex está marcada pola traxedia. A paraestatal tivo nos últimos anos gravísimos problemas de seguridade que acabaron en catástrofes que afectaron a vidas humanas, a infraestruturas e ao medioambiente, e que supuxeron para a petroleira un sobrecusto millonario en indemnizacións.

Velaquí unha cronoloxía dos accidentes máis graves sufridos por Pemex na historia recente desta compañía, fundada en 1938:

Torre Pemex, sede central da empresa paraestatal mexicana | Fonte: *Eneas*

- O 31 de xaneiro de 2013, produciuse unha forte explosión na sede central de Pemex na capital de México que causou 37 mortos e 126 feridos. Segundo unha información recente do xornal The New York Times, citando fontes departamentais do seu país, a explosión foi causada por unha bomba, máis a versión oficial do Goberno mexicano foi que o estoupido se produciu por unha "acumulación inexplicábel de gas, posíbelmente metano". O diario neoiorquino acusou ás autoridades mexicanas de interromper a participación de axentes da Oficina de Alcohol, Tabaco, Armas de Fogo e Explosivos de Estados Unidos que foran convidados a participar nas investigacións. Segunto o diario, as autoridades mexicanas fixeron todo o posíbel por impedir a investigación e "apresurar a conclusión de que a explosión foi un accidente".

- O 18 de setembro de 2012, rexistrouse unha explosión e un incendio nunha pranta de gas de Pemex Exploración e Produción (PEP), situada a 19 quilómetros de Reynosa, na zona nororiental do Estado de Tamaulipas, e que deixou un total de 30 mortos e decenas de feridos.

- O 19 de decembro de 2010, unha fuga de combustíbel, unha explosión e un incendio nun oleoducto de Pemex na poboación de San Martín Texmelucan, no Estado de Puebla, causaron 30 mortos e 52 feridos, ademais de 5.000 evacuados e 80 casas afectadas.

- O 23 de outubro de 2007, dúas plataformas mariñas colisionaron no Golfo de México, cun saldo de 18 persoas mortas e dúas desaparecidas, e houbo unha das maiores fugas de cru dun pozo petroleiro.

- O 17 de outubro do 2006, a explosión e incendio do buque tanque 'Quetzalcóatl', ancorado na Terminal Marítima de Pajaritos, deixou 8 mortos, un desaparecido e 14 feridos.

- O 18 de novembro de 1998, o choque de dous helicópteros que transportaban persoal de Pemex ás plataformas petroleiras nas costas do Estado de Campeche, no Golfo de México, deixou un saldo de 22 mortos.

- O 22 de abril de 1992, en Guadalajara, capital do estado de Jalisco, unha fuga de gasolina dun ducto de Pemex verteuse ao subsolo e ao sistema de drenaxe, o que causou unha explosión que deixou 210 mortos.

- O 19 de novembro de 1984, na peor traxedia na historia de Pemex, a explosión dun depósito de gas en San Juanico, no Estado de México, veciño ao Distrito Federal, deixou, segundo fontes oficiais, medio milleiro de mortos, aínda que de xeito extraoficial se falou de máis de 2.000.

Nun correo ao que tivo acceso GC, intercambiado polos analistas da axencia de intelixencia global Stratfor o 14 de outubro de 2010, estes apuntaban aos graves problemas de seguridade que existen en Pemex. Así, recordaban que "a seguridade nas operacións de perforación non é un punto forte para Pemex (os accidentes son bastante comúns)".

Esta apreciación publicábase tras a explosión na plataforma 'Deepwater Horizon' da compañía British Petroleum (BP), no Golfo de México, que ocasionou un enorme derrame e unha catástrofe medioambiental colosal. Isto empurrou a Pemex primeiro a axudar a BP e logo a revisar o seu programa de exploración e produción para incorporar medidas de prevención de accidentes; dous anos máis tarde, en 2012, ambas as dúas empresas asinaban un paradoxal acordo polo que Pemex contrataba a asesoría de BP para a xestión de catástrofes e control de derrames.

Corrupción, narcotráfico e secuestros

Executivos corruptos e empregados de Pemex a soldo das redes do narcotráfico escribiron nos últimos anos os capítulos máis escuros da paraestatal mexicana, na que a opacidade informativa foi un imperativo. De feito, a axencia Reuters, que nos últimos anos fixo importantes pesquisas sobre os vínculos entre as bandas criminais e empregados de Pemex, xa denunciou en máis dunha ocasión que a empresa non permite aos seus contratistas e traballadores falar cos medios de comunicación sobre os problemas de seguridade e corrupción que afectan á paraestatal; por iso, boa parte das informacións que se veñen recollendo sobre Pemex acostuman a ser relatos de testemuñas directas protexidas polo anonimato.

"Pemex rezuma corrupción"

"Cos fondos do monopolio petroleiro estatal mexicano Pemex se pagaron nos últimos anos tratamentos de liposucción para a esposa dun alto executivo da compañía, a campaña dun candidato á Presidencia, os contratos coas empresas que enfrontan accións legais e os caprichos dos dirixentes sindicais que non están obrigados a dar conta dos seus gastos". Así comezaba o xornalista Diego Cevallos unha información publicada o 7 de maio de 2008 pola axencia Inter Press Service (IPS) titulada "Pemex rezuma corrupción".

"Pemex é unha lata de bechos Se fas algo ben, van a por ti. Se calas sobre algunha irregularidade, cho recompensan. E se participas na corrupción, saes beneficiado", recollía Cevallos dunhas declaracións dun traballador da paraestatal.

"Miles de millóns de dólares pérdense na corrupción que, segundo os observadores, está profundamente arraigada nunha administración opaca afogada pola burocracia e os intereses políticos e económicos creados", proseguía o xornalista.

O artigo advertía dunha "percepción continua da opacidade, a corrupción e a ineficiencia en Pemex, unha empresa que é o botín de políticos e contratistas por igual, dixo o analista petroleiro David Shields".

"Trátase dunha sociedad secreta que opera lonxe do escrutinio público e que xenera enormes cantidades de diñeiro que se distribúe co criterio do sistema político", continuaba o analista.

Entre os casos de corrupción destaca, por exemplo, o que protagonizou en xullo de 2007 o ex-director de Pemex, Raúl Muñoz, sancionado cunha multa de 80 millóns de dólares e prohibición de exercer cargos públicos por dez anos polo "mal uso dos fondos e a transferencia ilegal de máis de 170 millóns de dólares ao sindicato de traballadores petroleiros".

"Muñoz tamén utilizou 12.500 dólares dos fondos de Pemex para pagar dúas cirurxías de liposucción para a súa esposa", recordaba Cevallos.

"A sona da corrupción na compañía petroleira está tan profundamente arraigada, que a finais de 2007 un grupo de artistas da estafa non tivo problemas para vender a unhas 200 persoas os documentos que supostamente garantían que serían postos na nómina da empresa", denunciaba o artigo publicado en IPS.

En marzo de 2010, o empresario Ricardo Salinas Pliego, dono de Televisión Azteca e un dos homes máis poderosos de México, lanzou duras críticas contra Pemex nunha xuntanza da Sociedade de Periodistas e Editores Financeiros de Estados Unidos, na cidade de Phoenix (Arizona). O millonario mexicano acusou á paraestatal de estar "fóra de calquera supervisión", de modo que nesa empresa "todo é escuro e así está ben (*nice and dark*)".

Noutro correo electrónico da axencia de intelixencia global Stratfor recórdase que en 1994, o célebre político mexicano Andrés Manuel López Obrador se postulou para o cargo de gobernador de su Estado natal, Tabasco, e perdeu ante Roberto Madrazo, candidato do Partido Revolucionario Institucional (PRI) nas eleccións do 2 de xullo. Segundo os analistas, "Madrazo sobrepasara os límites permitidos na campaña de 1994 e López Obrador aproveitou a ocasión para denunciar o fraude e comezar un movemento de 'resistencia civil'. Dirixiu os seus grupos de simpatizantes para bloquear a entrada de varias plataformas petrolíferas e outras instalacións de Pemex en Tabasco durante varios meses. Tamén organizou manifestacións e caravanas a Cidade de México. López Obrador non tivo éxito na reversión da elección, pero gañou a suficiente visibilidade para posicionarse como o próximo presidente nacional do Partido da Revolución Democrática (PRD) e logo como alcalde da Cidade de México".

A conexión galega

O 24 de febreiro de 2008, Andrés Manuel López Obrador acusou ao entonces secretario de Gobernación, Juan Camilo Mouriño —o fillo do presidente do Celta de Vigo, que morreu nun estraño accidente de aviación na capital mexicana—, de tráfico de influencias benificiando empresas da súa familia con contratos outorgados por Pemex cando desempeñaba o cargo de asesor na Subsecretaría de Electricidade da Secretaría de Enerxía en 2003 e 2004.

Entre os anos 2006 e 2010 foran detectados un total de 153 casos de empresas defraudando en Pemex Exploración e Produción (PEP), a maior filial do grupo Pemex, das cales só catro era estranxeiras. E de todos eses casos, 57 foron detectados en 2010, durante a Administración do presidente Felipe Calderón.

En maio de 2008 informábase da existencia dunha rede de corrupción entre funcionarios de Petróleos Mexicanos e provedores da paraestatal que viña funcionando desde o ano 2006. Os subornos a través de compras irregulartes eran algo habitual nesta rede que afectaba a Pemex Petroquímica (PPQ). Finalmente, doce funcionarios foron sancionados pola Secretaría da Función Pública (SFP).

A finais de agosto de 2011, novos escándalos de corrupción salpicaron a Pemex. Deputados federais do PRI e PT esixiron á Procuraduría General de la República (PGR) e á Auditoria Superior da Federacion (ASF) investigar os contratos por máis de 42 millóns de dólares outorgados presuntamente de forma ilegal á empresa KBC Advanced Tecnologies, Inc por parte de Pemex-Refinación, informaba Milenio.

"O coordinador lexislativo do Partido do Traballo (PT) en San Lázaro, Pedro Vázquez González, dixo que Pemex-Refinación se converteu nunha empresa onde hai un manexo financeiro e de contratos con máis irregularidades, opacidade e presúmese maior corrupcion", explicaba o medio mexicano.

De acordo cun informe lexislativo, en decembro de 2010 xa foran "inhabilitados e sancionados 14 funcionarios de Pemex-Refinacion" con multas por valor duns 315 millóns de euros por dano patrimonial paraestatal.

En outubro de 2011 saltou un novo caso de corrupción nas altas esferas de Pemex. A Secretaria da Funcion Publica (SFP) sancionaba a catro directivos de Petréleos Mexicanos por provocar danos millonarios á paraestatal entre os anos 2008 e 2009. A prensa mexicana informaba de que SFP destituíra a María del Rocío Cárdenas Zubieta, directora xeral de PMI, Comercio Internacional SA de CV, filial de Pemex, por un período de 10 anos para traballar no Goberno Federal, e impoñíalle unha multa duns 18 millóns de euros, unha das sancións mais altas que se impuxeron en Mexico, como parte dunha investigacion que realizou esa dependencia por diversos actos de corrupcion.

Pola súa banda, Alejandro Tello, xerente comercial de Gasolinas e Compoñentes de PMI, foi multado cuns 757.000 euros; César Elías Covarrubias, encargado de despacho da Dirección Comercial de Refinados de PMI, sancionado con 5.362.000 euros; e Alberto Olimón Salgado, subdirector Comercial de Gasolinas e Compoñentes de PMI, cuns 10.765.000 euros.

Os catro directivos foran acusados de facilitar "descontos excesivos e inxustificados" na venda da gasolina denominada "cóquer" a favor das empresas Trafigura e Gunvor, líderes na compra e venda de hidrocarburos a nivel internacional. O dano ocasionado a PMI Comercio Internacional por unha serie de operaciones comerciais realizadas polos funcionarios sancionados ascendía a 1,75 millóns de dólares, mentres que o prexuízo para a paraestatal foi de 24,3 millóns de dólares.

Porén, o secretario de Enerxía, Jordy Herrera Flores, e o conselleiro profesional de Pemex, Fluvio Ruiz, defenderon á ex-directora da filial PMI, malia que Pemex Petroquímica (PPQ) fora tamén vítima desa filial, onde igualmente estivo implicada a holandes Trafigura, informaba a prensa mexicana. A recomendacion que lle fixo PMI a PPQ a mediados de 2009 foi manter o contrato coa holandesa Trafigura para a compra de naftas aos prezos que tiñan pactados, que representaban un sobrecusto do 66.4%.

A corrupción está inoculada en Pemex. Tanto é así, que hai apenas unha semana a publicación El Financiero denunciaba que "entre 2006 a 2012 Petróleos Mexicanos entregou ao sindicato de traballadores petroleiros 169,5 millóns de pesos polo pago do desfile do aniversario do Día do Traballo e os seus gastos administrativos asociados", cando este evento non se celebra desde o ano 1995.

Segundo El Financiero, "a entrega dese diñeiro forma parte dun convenio establecido no marco do contrato colectivo de traballo do sindicato petroleiro" que "non foi ha modificado" e o manexo destes recursos permanece na opacidade".

Con todo, Pemex sempre aduciu que os traballadores corruptos son unha pequena parte dos case 150.000 empregados da paraestatal petroleira, e sempre sinalou como principais culpábeis as redes do crime organizado.

Infiltracións do narcotráfico e do crime organizado

As redes do narcotráfico e o crime organizado infiltráronse en Pemex coa colaboración de empregados da empresa, desde a súa base até altos cargos da paraestatal. Os casos son múltiples. Por exemplo, no ano 2009, Eduardo Mendoza Arellano, lexislador federal que encabezaba a Comisión de Enerxía da Cámara de Deputados mexicana, asumía que a organización criminal Los Zetas actuaba como un "goberno paralelo", que "dominaba vastas extensións de canos, dende as estradas até as mesmas portas das compañías petroleiras", informaban Steve Fainaru e William Booth no xornal Washington Post en decembro daquel ano.

"Los Zetas gañan millóns de dólares por 'gravar' os oleoductos", explicaban os xornalistas, que apuntaban aos vínculos desta organización criminal con Petróleos Mexicanos: "Los Zetas traballan a miúdo con antigos empregados de Pemex, segundo Ramón Pequeño García, xefe de operacións da loita contra as drogas no Ministerio de Seguridade Pública de México". O perfil destes ex-traballadores é o de "persoas altamente cualificadas que teñen coñecementos técnicos para extraer petróleo dos oleoductos" e que se puxeron "baixo o control de Los Zetas", explicaba Pequeño.

Segundo o analista de enerxía George Baker, cuxa oficina se atopa en Houston, "a maioría da xente que sabe como se fai isto está en Pemex ou son ex-traballadores de Pemex, porque son operacións de alta tecnoloxía".

Karen Hooper, analista para América Latina de Stratfor, comentaba nun correo ao que tamén tivo acceso este xornal, enviado ao seu departamento o 3 de agosto de 2009, que "a relación entre funcionarios de Pemex e Los Zetas plantexa preocupacións de seguridade e protección, tanto para excutivos de Pemex como para os das compañías petroleiras estranxeiras que podan facer tratos con Pemex".

Secuestros

En novembro de 2010, Mark Stevenson asinaba unha noticia de Associated Press (AP) na que se informaba de que os *cárteles* da droga estaban interrompendo servizos básicos en México. O artigo arrincaba co caso de cinco traballadores de Pemex que de camiño a unha planta de gas do Goberno preto da fronteira con Texas desapareceran seis meses atrás. O xornalista lembraba que "homes enmascarados, ao parecer membros dun *cártel* da droga que opera alí, xa advertiran aos empregados de Petróleos Mexicanos que xa non se lles permitía entrar naquela área".

"Cos asasinatos e desaparicións para facer valer a súa autoridade, os *cárteles* da droga de México empezan a interferir nos petos do país a través das actividades cotiáns do Goberno, mantendo aos traballadores fóra do seu territorio e interrompendo algúns dos servizos máis básicos. [...] están bloqueando as entregas de gasolina, cheques de pensión, asistencia agrícola e outros servizos para os mexicanos.", explicábase. Porén, e malia as denuncias cidadás, as autoridades federais dicían que "estes eran incidentes aillados" e negaban que existira calquera zona do país onde o Goberno non poidese operar.

A axencia Reuters daba a mediados de 2011 unha cifra de 17 vítimas en Pemex a mans das bandas criminais, desde 2005.

A desaparición dos traballadores de Pemex e a intervención dos narcotraficantes na paraestatal mexicana tamén suscitaron máis comentarios en Stratfor. O 10 de setembro de 2010, noutro correo dos analistas desta axencia de intelixencia ao que accedeu GC, comentábase que "Pemex nunca vería a luz do día coa corrupción tan firmemente arraigada en todos os niveis da empresa".

Ao tempo que o Goberno negaba as evidencias, a propia empresa paraestatal Pemex recoñecía que os secuestros eran un "problema xeral", en palabras do seu por entón director xeral, Juan Suárez Coppel. Stevenson recordaba que "un total de 10 empregados ou subcontratistas de Pemex foron secuestrados en catro Estados mexicanos en 2010, en comparación con só un en 2009, dous en 2008 e tres en 2007".

Con todo, Pemex non estivo pola labor de informar claramente sobre as súas estimacións das perdas que lle viñeron causando estes ataques, segundo o artigo publicado por AP. "A empresa non puido dicir que sucedeu coas vítimas, ou a cantidade da producción que se perdera a causa dos problemas de seguridade nos Estados fronteirizos como Tamaulipas e Nuevo León, e dos Estados da costa do Golfo Veracruz e Tabasco", relatábase no artigo.

Así, a empresa limitouse a responder ambigüamente que houbo "unha serie de situacións na parte norte de Tamaulipas e en Nuevo León que foron difíciles de manexar", en palabras escritas a AP por parte de Carlos Morales Gil, director de Pemex Exploración e Produción.

En abril de 2010 produciuse outro secuestro que tivo moito impacto na opinión pública mexicana, o do executivo Néstor Martínez, que xestionaba unha unidade de produción de enerxía en Tabasco. Martínez foi posto en liberade un mes despois, supostamente tras pagarse o seu rescate. O seu non foi algo anecdótico, todo o contrario. Reuters destacaba que unha "onda de secuestros de executivos de Pemex sacudiu a industria petroleira nun país onde os *cárteles* da droga e as bandas do crime organizado están cada vez máis asustando aos inversores estranxeiros". De feito, Martínez era o cuarto executivo de Pemex secuestrado polas bandas criminais entre marzo e abril de 2010, informaba Reuters.

En novembro de 2010, contabilizáronse até dez secuestros de traballadores de Pemex nos estados de Tabasco e Chiapas durante ese ano, dos declarados oficialmente. Porén, os informes non oficiais din que houbo en realidade cando menos 30 persoas secuestradas só en Chiapas e "decenas máis "ameazadas regularmente", informaba a prensa mexicana.

Roubos millonarios

En xuño de 2011, a axencia Reuters informaba de que Pemex iniciara unha demanda contra once empresas de Estados Unidos pola compra de até 300 millóns de euros en combustíbel roubado por bandas de narcotraficantes e de contrabando na fronteira México-Estados Unidos. A paraestatal mexicana aducía que estas empresas conspiraran con criminais mexicanos para falsificar documentos e o contrabando de gas natural condensado roubado a Pemex. "Os xacementos da cunca de Burgos de Pemex que se extenden polos Estados mexicanos norteños de Tamaulipas, Nuevo León e Coahuila foron ameazados polos poderosos *cárteles* da droga que se ramifican con novos manexos ilegais en busca de maiores ingresos".

Finalmente, un puñado de executivos estadounidenses se declararon culpábeis. Entre estes, Tim Brink, ex-director xeral de Continental Fuels, confesou na súa declaración final que foran funcionarios de Pemex quen lle deran os contactos cos grupos criminais que roubaban á empresa paraestatal.

Un informe propio de Pemex recoñecía que só entre xaneiro e abril de 2011 foran roubados 969.120 barrís de combustíbel, valorados nuns 190 millóns de euros, a través de conexións ilegais aos canos da compañía, informaba o xornal mexicano El Universal. Pemex xa era obxectivo prioritario das redes criminais. O volume roubado nos catro primeiros meses de 2011 era un 49% maior respecto ao substraído durante o mesmo período en 2010 (estimado en 648.257 barrís) e era máis dos 800.000 barrís diarios de gasolina que se consumen en México.

Un mes despois, en xullo de 2011, Reuters destapaba que cando menos 97 traballadores e sete contratistas de Pemex estaban vinculados aos roubos de combustíbel en México dende o ano 2000.

"Os traballadores corruptos colaboran coas bandas do crime, algúns con vínculos con poderosos *cárteles* do narcotráfico, para roubar camións cisterna ou sifóns de gas, petróleo cru e combustíbel de aviación", explicaba a axencia de noticias, que salientaba os "coñecementos de enxeñería e do funcionamento interior da empresa" destas persoas.

O impacto destes roubos na economía mexicana é brutal, xa que "arredor dun terzo dos orzamentos do Goberno depende dos ingresos do petróleo", sinalaba Reuters, que estimaba nuns 600 millóns de dólares as perdas que viña acumulando a empresa desde 2010 polos roubos. Só en 2008, Pemex deixou de ingresar cerca de 715 millóns de dólares polas subtraccións e en 2009, outros 350 millóns. En 2010, a empresa perdeu uns 190 millóns de euros polos roubos, segundo datos aportados polo seu director xeral.

"Estes roubos son ademais un golpe simbólico e financeiro para o Goberno mexicano. Os impostos pagados por conta de Pemex son o 40 por cento do orzamento federal", incidían pola súa banda os xornalistas de The Washington Post. Reuters tamén sinalaba a xustiza mexicana como un problema para acabar coa impunidade dos criminais, xa que "a debilidade do sistema xudicial de México fai difícil a súa condena". Así, a axencia subliñaba que desde o ano 2000 até agosto de 2010 houbera 2.600 denuncias por roubos e só se ditaran 15 sentencias.

O número de tomas clandestinas de ductos cuadruplicouse desde 2004, cando se detectaron 102, deica o ano 2009, cando foron localizadas 462, segundo os datos aportados por Pemex. A empresa estimou que lle roubaran 8.432 barrís de produtos derivados do petróleo por día no ano 2009. Porén, nun correo electrónico do 16 de marzo de 2011 entre analistas da axencia de intelixencia estadounidense Stratfor, co asunto "Cartels and oil", a súa experta Sylvia Longmire consideraba que os datos feitos públicos por Pemex da súa perda de combustíbel polos roubos eran "cifras rebaixadas".
Un ex-contratista de Pemex recoñeceu a Reuters que sempre existiu unha alianza entre traballadores da paraestatal e os criminais, e que a rede de corrupción afectou estes últimos anos "a grupos en todos os niveis" e isto, segundo o confidente de Reuters, foi sempre *vox populi* en Pemex. Hai que salientar o medo a represalias que teñen quen denuncian estes casos de corrupción en Pemex e roubos do crime organizado, e polo tanto prefiren gardar o anonimato.

A empresa fixo fortes investimentos extras nos últimos anos para asegurar o seu negocio, instalando sistemas de control sofisticados, incluíndo a vixilancia por satélite, cámaras e medidores de circuítos pechados, cos que conseguira reducir os roubos de combustibel nun 66% entre 2008 e 2010. Ao tempo, os criminais foron tamén perfeccionado os seus sistemas, técnicas e redes de contactos, aumentando nun 55% as tomas de ductos ilegais durante ese tempo. E así, os roubos volveron dispararse en 2011 polos vínculos entre traballadores da empresa e o crime organizado.

Juan José Suárez, director xeral de Pemex entre 2009 e 2012, xa estimaba hai catro anos que a empresa tería que gastar "centos de millóns de dólares" nos seguintes tres anos para defender os seus ductos.

Como o crime organizado se apoderou de Pemex

A xornalista mexicana Ana Lilia Perez é a autora do libro 'O cártel negro: como o crime organizado se apoderou de Pemex', publicado a finais de 2011 por Grijalbo. Neste libro, froito dunha investigación, destápase a infiltración das redes do narcotráfico en Pemex mediante unha complexa trama de complicidades e corruptelas nas que "participaron directivos, contratistas e traballadores da paraestatal para permitir o roubo, o saqueo e a impunidade". Desde o ano 2012, a xornalista vive no exilio, ameazada presuntamente por funcionarios públicos.

Velaquí algúns extractos do libro:

(...) Como encargado da operacion de pozos, a funcion de Rogelio Gutiérrez consistia en recibir e rexistrar en bitácoras as descargas dos autotanques, e bombear o condensado da estacion de recoleccion aos ductos. Ese traballo facíao desde 1996, ano no que ingresou a traballar en Pemex asignado, precisamente, ao Activo de Producion Burgos Reynosa, de maneira que coñecía a area e os procedementos como a palma da súa man.

Aquela noite parecia que todo funcionaba segundo os procedementos cotiáns, pero en realidade non era así. No peto dereito do seu pantalon, o empregado de Pemex traia unha pistola Raven Arms modelo P25, numero de serie 467829, cromada con cachas de madeira, catro cartuchos útiles no cargador e un na recámara. Estaba armado no seu horario de traballo porque o que aquela noite facía Rogelio era abastecer un dos cargamentos de condensado que ilegalmente se sacaban de Burgos para traficarse a Estados Unidos, onde os contrabandistas o vendían a grandes e prestixiosas compañias petroleiras, como a alemá BASF e Murphy, de orixe estadunidense, as cales empregaban o hidrocarburo para a formulacion de gasolinas. Polo menos desde 2006, na Union Americana moitos consumidores adquiriron gasolinas formuladas con materia prima roubada a Pemex e traficada coa proteccion dos *cárteles* da droga mexicanos.

Coa implicacion de empregados de Pemex e dos seus contratistas iniciouse a subtracción de condensado da Cunca de Burgos, que a partir de 2006 comezou a introducirse de contrabando en territorio estadunidense, a mans de redes internacionais nas que o Servizo de Inmigracion e Control de Aduanas de Estados Unidos (ICE, polas súas siglas en ingles) descubriu a participacion da dupla que formaban o cartel do Golfo e Los Zetas, chamada A Compañía.

A Compañía era dirixida por un 'triunvirato' integrado por Antonio Ezequiel Cardenas Guillén, alias Tony Tormenta, irmán de Osiel Cardenas; Jorge Eduardo Costela Sanchez, o Coss, o Dobre X ou Dous Equis, e Heriberto Lazcano Lazcano, o Lazca, o Verdugo, o Licenciado, ou Zeta-3, quen asumio o liderado dos Zetas trala caída do seu xefe fundador Arturo Guzmán Decena, Zeta-1, ocorrida en novembro de 2002 en Matamoros.

A incursion do *cártel* no negocio dos hidrocarburos sumoulle considerábeis ingresos para soster a custosa estrutura coa que entón controlaba o trafico de drogas desde Colombia e Venezuela cara a México e Estados Unidos. Administraban redes de narcomenudeo, xiros negros, tráfico de indocumentados e piratería en case a metade do país, todos os estados do Golfo, máis Nuevo León, San Luis Potosí, Chiapas, parte de Michoacán e o Distrito Federal. E mesmo mais aló do territorio mexicano, nos departamentos fronteirizos de Guatemala no sur, e no norte, en estados como Texas e cidades importantes como Atlanta, Georgia, a que o Departamento de Xustiza de Estados Unidos identificou como epicentro das operacións do cartel no veciño pais do norte.

(...) Desde 2006, cando se rexistraron os primeiros roubos e as importacións ilegais a Estados Unidos, o Goberno mexicano tivo coñecemento diso. Os directivos de Pemex foron informados do que sucedía no activo de produción mais importante do noreste mexicano. A área de intelixencia da paraestatal notificoullo, pero eles calaron e decidiron clasificar cada un dos roubos como informacion reservada por 12 anos.

(...) Sóubose que non se trataba de roubos illados nin cometidos pola delincuencia común, senón que os *cárteles* da droga estaban detrás do negocio, un feito que xa se puxera de manifesto nas primeiras confrontacións entre elementos da Xerencia de Servizos de Seguridade Física e membros do *cártel* do Golfo.

(...) Nas poucas ocasións que chegaron a instancias xudiciais os fretadores argumentaron que os seus choferes actuaban de forma individual; con todo, eses condutores tiñan o apoio xuridico dun avogado que os poñía na rúa en menos de 24 horas. Mesmo, ás veces, o defensor que representaba ao chofer era o mesmo que defendía aos empregados de Pemex detidos *in fraganti* na subtraccion ilicita. Un deses casos foi precisamente o do cargamento que preto da medianoite do 2 de agosto de 2006 saíu nunha pipa de Intertransports.

(...) Nunha espiral de corrupcion e complicidades, os roubos fixéronse cada día máis frecuentes e a calquera hora do día. En só uns meses o mercado esixía tanto produto, que non era suficiente o persoal de Pemex que abstecía os pedidos. Entón comezaron a asaltar as pipas propiedade da paraestatal e as que esta dependencia contrataba con terceiros, para levar o condensado dos tanques de almacenamento ás terminais e centros de produción.

Desde a chamada fronteira chico ou ribereña, en Tamaulipas, e ata Piedras Negras, en Coahuila, ao longo de camiños e fendas de toda a Cunca de Burgos, os comandos armados, vestidos de negro e enpuzados, permanecian apostados, prestos ao atraco, en canto o falcón lles notiticaba que o cargamento ía en camiño. Os informantes usaban a rede de comunicacion interna de Pemex, que funciona via radio *trunking*, un sistema móbil para un grupo privado de usuarios, quen poden compartir datos de forma automática e organizada. Para conectarse a esa rede interna non basta con ter os aparellos, senón que se requiren os codigos de chamada; os comandos criminais obtivéronos.

(...) A partir de que comezaron as primeiras subtraccións e envíos a Estados Unidos, o contrabando de condensado creceu rapidamente. Alcanzou tal nivel, que xa en 2007, segundo cifras internas de Pemex, o 40% de todo o hidrocarburo que producía a Cunca de Burgos se substraía ilegalmente e se vendia no mercado negro, basicamente en territorio estadounidense.

En 2007, o primeiro ano de goberno de Felipe Calderon, as tomas clandestinas montadas dentro da rede de ductos de Pemex alcanzaron o maior número rexistrado na historia da petroleira: 323, case unha diaria. Catro anos despois, a cifra multiplicábase a máis de tres tomas en promedio por día. Para 2011, só por esa vía o roubo de hidrocarburos incrementárase un 300% e quizá moito máis, se consideramos que só se contabilizan as tomas detectadas, mentres que hai outras que non están situadas e ordénanse permanentemente sen posibilidade de ser clausuradas.

Así, o volume dos hidrocarburos substraídos a traves desas tomas clandestinas alcanzou niveis exorbitantes. Os números oficiais que Pemex deu a coñecer en setembro de 2011 revelan que os ordenadores de ductos (que inclúen oleoductos, poliductos e gasoductos) substraen en promedio 20.000 barrís de hidrocarburos diariamente. A cifra equivale a mais de 3 millóns de litros de petrolíferos. Dito doutro xeito, o promedio da subtraccion clandestina ascende a 200 pipas diarias. Trátase particularmente de gasolina, aínda que o roubo de petroleo cru —documentado neste libro— tamén vai ao alza; son perdas patrimoniais que a Comision de Xustiza da Cámara de Deputados calculou en 1.300 millóns de pesos mensuais.

Tamén en setembro de 2011, o Pleno da Cámara de Deputados aprobou endurecer as penas polo roubo ou aporoveitamento de petróleo cru, hidrocarburos refinados, procesados e os seus derivados de ductos, equipos ou instalacións de Pemex. Asi, mediante reformas ao Codigo Penal, a Lei Federal Contra a Delincuencia Organizada e o Código Federal de Procedementos Penais, estableceuse como delincuencia organizada o roubo a ductos de Pemex.

Considerado xa como delito grave, aprobáronse sancións de 8 a 12 anos de prisiín e de mil a 12 mil dias de salario mínimo de multa a quen substraia hidrocarburos propiedade de Pemex, e penas de dous anos de cárcere e ata 500 días de salario mínimo de multa a quen posúa ou resgarde de xeito ilícito calquera hidrocarburo. A penalidade aumenta a 18 anos cando os implicados sexan traballadores ou funcionarios da paraestatal.

(...) En realidade, hai moito que o problema pasou ás autoridades. En México ata as leis mais avanzadas son letra morta cando o que impera é a corrupcion. Considérese, por exemplo, a efectividade real da PGR nos casos abertos por roubo ou subtraccion de hidrocarburos: só catro de cada cen derivaron en auto de formal prisión.

Para desfalcar a Pemex co seu ouro negro, non sempre é necesario mancharse as mans, polo menos non literalmente. Asi o demostrou a directora xeral de PMI Comercio Internacional —a subsidiaria encargada das vendas de Pemex en Estados Unidos, Europa e Asia—, Rocío Cárdenas Zubieta, unha das funcionarias de maior nivel na paraestatal. Xunto con outros tres funcionarios (o subdirector comercial de Gasolinas e Compoñentes, Alberto Olimon Salgado; o xerente comercial de Gasolinas e Compoñentes, Alejandro Tello Winniczuk; e o encargado de despacho da Dirección Comercial de Refinados, César Elías Covarrubias Prieto), Cárdenas Zubieta operaba unha rede de corrupción que mediante "descontos" lle vendian gasolina cóquer mexicana a prezo de ganga ás transnacionais Trafigura e Gunvor, as compañías de compra-venda de hidrocarburos máis grandes do mundo.

A SFP auditou as vendas que lle fixo a representante da paraestatal ás dúas compañías de xaneiro de 2008 a xaneiro de 2009, e encontrou que eses "descontos excesivos e inxustificados" causaron un dano patrimonial de 1.75 millóns de dólares e un prexuízo de 23.3 millóns de dólares, calculado o primeiro a partir da diferenza entre os ingresos pola venda e os custos do combustíbel; e o segundo a partir do monto que Pemex recibise de vender a gasolina a un prezo adecuado.

Polo demais, en outubro de 2011 Cárdenas Zubieta foi inhabilitada para servir na administración pública por 10 anos e obrigada a pagar unha multa de 284 millóns de pesos.

Esa mesma funcionaria participou noutras cuestionadas operacións dos directivos de Pemex, como a operación de compra de accións de Repsol para aumentar a participacion de Pemex, aínda que non foi a responsábel de aprobala. Operación que en 2011 puxo en xaque ao director xeral de Pemex, Juan José Suárez Coppel, ao evidenciarse o nivel de discrecionalidade en operacións de tal magnitude.

As demoledoras cifras que Pemex fixo públicas en setembro de 2011 puxeron en evidencia, oficialmente, que o combate ao roubo de combustíbeis é outra batalla perdida por Felipe Calderón, unha batalla onde o que esta en xogo é unha grande parte do gasto público do país, 40% do PIB nacional.

As reformas á lei apenas se estan aprobando, cando hai tempo que a mafia se fusionou ao quefacer cotián da industria petroleira.

Entre a accion gobernamental e a situación real hai unha distancia de anos luz. Os lexisladores endurecen penas sen esclarecer primeiro a maraña de complicidades que fixeron do *cártel* negro unha criatura invencíbel, que emerxeu desde as entrañas mesmas da industria do petróleo.

Ata hai uns anos, Pemex era o escaparate do nacionalismo mexicano, da dedicacion dos seus traballadores, do amor á camiseta. A ambición polo diñeiro fácil degradouno todo. Hoxe son negocios, só negocios. Baixo a lóxica do *business*, practicamente desde o máis alto funcionario ata o máis modesto dos obreiros esta disposto a venderlle a súa alma ao diaño, ou de xeito mais simple e directa: a aliñarse co maná.

Actualmente, as operacións ilegais en Pemex alcanzan tal nivel, que custa traballo saber en cantos dos negocios que oficialmente fai a paraestatal están presentes as operacións financeiras do crime organizado.

Con estes antecedentes, o normal é preguntarse que futuro lle espera ao estaleiro vigués Hijos de J. Barreras en mans dunha empresa de dubidosa reputación e intervida, por un lado, polos intereses partidistas, sindicalistas e nacionalistas mexicanos, e polo outro, polo crime organizado; dúas empresas, dous símbolos de dous países con distintos trazos pero condenadas a fusionarse para a súa salvación.

ANEXO XVIII: Publicación 10 de los correos de Stratfor.

Pemex (II): opacidade, creba técnica e deslocalización de Barreras

A mala xestión de Petróleos Mexicanos, en creba técnica, as irregularidades nas contratacións, a polémica e frustrada experiencia da paraestatal mexicana como accionista de Repsol e a súa teima por tomar a tecnoloxía doutras empresas poñen en dúbida as súas intencións para co estaleiro vigués Hijos de J. Barreras. GC ofrece as claves da estratexia agresiva de Pemex para levar o estaleiro galego a México.

- Pemex (I): corrupción, crimes e inseguridade no novo dono de Barreras
- A mala fama de Pemex na súa casa
- Axudar ao GC é agora máis doado e rápido

Por Alberto Quian | Vigo | 13/05/2013 | Actualizada ás 08:00

Petróleos Mexicanos non só está intervida pola corrupción e as redes do narcotráfico. A empresa paraestatal vén padecendo a incompetencia e neglixencias demostradas e documentadas dos seus xestores, que levaron a petroleira á creba técnica, cunha débeda bancaria descomunal de 48.000 millóns de euros.

Asteleiros Barreras, que pasarán a mans de Pémex | Fonte: *economiadigital.com*

A produción de petróleo de Pemex caeu estrepitosamente nos últimos anos e os atrancos da Constitución mexicana á apertura das portas a inversores estranxeiros condenaron á empresa pública a unha situación de declive agravada pola corrupción e os desmandos. Á crise financeira de Pemex hai que sumarlle as fendas tecnolóxica, de credibilidade e de legalidade nas que se afundiu a paraestatal.

As irregularidades nas contratacións forman parte do *normal* funcionamento desta empresa, cualificada pola propia prensa do seu país e en diversos informes como unha compañía opaca na que non hai uns mínimos de transparencia. Ademais, Pemex leva tempo padecendo un subdesenvolvemento tecnolóxico que levou aos seus xestores a priorizar unha estratexia agresiva de investimentos en empresas foráneas para poñer en marcha a transferencia tecnolóxica que precisa Pemex para mellorar os seus desfasados sistemas e infraestruturas. Este será precisamente o obxectivo de Pemex coa toma de control do 51% do capital do estaleiro vigués Hijos de J. Barreras.

Obxectivo prioritario: a transferencia tecnolóxica

As mínimas reformas que se aprobaron no Congreso mexicano no ano 2008 en materia de enerxía foron encamiñadas principalmente a aumentar a eficiencia de Pemex e permitirlle a contratatación de compañías foráneas, esperando ter maior acceso aos coñecementos e experiencias tecnolóxicas dos que carece a mexicana. Porén, os expertos da axencia de intelixencia global Stratfor xa viñan advertindo de que os principais campos de extracción en terra, como Cantarell, estaban xa en declive desde hai anos, o que plantexaba "interrogantes sobre se as reformas poderían ser moi escasas e tardías".

Torre Pemex, sede central da empresa paraestatal mexicana | Fonte: *Eneas*

Todos os analistas veñen coincidindo en sinalar o subdesenvolvemento tecnolóxico que arrastra Pemex, que lle impide poñer en marcha plans de explotación para aumentar a súa produtividade. Esas limitacións técnicas, a falta de *know-how*, xa as evidenciou o informe de Business Monitor International titulado 'Mexico oil & gas report Q4 2011', de outubro de 2011. Nunha análise DAFO (debilidades, ameazas, fortalezas e oportunidades), sinalábanse como unha clara ameaza para Pemex e, polo tanto, para as contas do Estado mexicano que engorda cada ano a paraestatal, a "caída a longo prazo da produción nacional de petróleo".

Neste mesmo informe alertábase da "opacidade" na que se desenvolve esta empresa, xa que as cifras que vén dando a paraestatal sobre as súas reservas "son cuestionadas por algúns analistas, debido ao monopolio de Pemex na avaliación de reservas".

"Segundo as estimacións independentes, en xeral, estas amosan cifras máis conservadoras. Porén, ambas as dúas partes están de acordo en que as reservas probadas de México están caendo constantemente a medida que os novos descubrimientos non poden compensar o envellecemento dos principais campos", explicábase neste documento.

O informe era categórico: "Pemex terá que formar alianzas con empresas petroleiras internacionais nun esfozo por gañar o acceso á tecnoloxía necesaria, do contrario a campaña de perforación da empresa podería levar moito máis tempo do esperado".

Perigo de deslocalización para Barreras

Unha vez feito público o acordo alcanzado para que Pemex se faga co control do 51% de Barreras e, polo tanto, obstente o poder absoluto sobre a empresa galega, os mexicanos non disimulan a súa intención de levar a cabo unha transferencia tecnolóxica completa que remataría coa deslocalización de Barreras. Existen os suficientes indicios para pensar que a medio prazo, Vigo podería dicir adeus a súa factoría, insgnia do naval galego, e resignarse a ver como os mexicanos levan e *muxen* a alfaia naval viguesa para *alimentar* as contas do Goberno do país azteca.

A prensa mexicana non encubre as intencións da paraestatal do seu país para co estaleiro vigués Hijos de J. Barreras. Pemex acabará transferindo ao outro lado do Atlántico, a medio prazo, o coñecemento tecnolóxico de Barreras para crear capacidade construtora de buques especializados en México, co fin de poder atender a demanda da empresa pública azteca, segundo recoñeceu a propia empresa mexicana.

É dicir, a incursión de Pemex en Vigo podería facer bo o refrán de "pan para hoxe e fame para mañá", xa que se dá por feito que os mexicanos desmantelarán e levaranse o estaleiro galego para facer fortes investimentos en México. A suma total será de 535 millones de euros para anovar a súa frota petroleira con cando menos 81 embarcacións para Pemex Exploración y Producción (PEP) e outros 51 buques para Pemex Refinanciación. Fontes de Pemex insisten en que os recursos que aportarán para a toma do 51% de Barreras proceden do orzamento destinado pola petroleira á compra dos floteis.

Se se cumpren os plans de Pemex, a deslocalización de Barreras non tardará en producirse.

Segundo Pemex, o obxectivo que persegue é transferir a medio prazo o coñecemento tecnolóxico de Barreras para crear capacidade construtora de buques especializados en México, concretamente na súa base de operacións de Ciudad del Carmen, no Estado de Campeche (suroeste da península de Yucatán), co fin de poder atender a demanda da paraestatal.

Con todo, tanto a Xunta como a patronal amosánse satisfeitos co acordo para que a petroleira mexicana controle Barreras a cambio da construción de dous buques hotel e restan importancia á transferencia tecnolóxica.

Pola súa banda, os sindicatos galegos esixen "transparencia" e na oposición, os socialistas temen que existan "cláusulas ocultas" no acordo entre Pemex e Barreras, mentres que os nacionalistas observan que a intención dos mexicanos é "apropiarse do capital tecnolóxico" do estaleiro vigués. O certo é que os aspectos máis sensíbeis do acordo son aínda confidenciais e pouco se sabe das condicións impostas polos mexicanos, algo que non sorprende se temos en conta que a opacidade forma parte da cultura empresarial de Pemex.

Creba técnica de Pemex e "problemas de opacidade e ética"

Os medios mexicanos falan de Barreras como unha "empresa en creba" sobre a que tomará o control Pemex co 51% do capital. Pero Pemex tamén é unha empresa en "creba técnica", como recoñece o analista da industria enerxética David Shileds na publicación Reforma. De feito, estímase que a débeda de Pemex coa banca acredora é colosal e ascende a uns 48.000 millóns de euros, dos cales preto de 38.000 millóns están atrapados en bancos estranxeiros e o resto en entidades mexicanas.

Shields lanza varias interrogantes que deben ser respondidas e dubida da capacidade de Barreras para satisfacer a demanda de Pemex:

> "Si, Hijos de J. Barreras podería construír cando menos uno dos floteis que Pemex Exploración y Producción (PEP) podería requirir para traballos en augas profundas. Pero Barreras non é unha compañía especializada en infraestrutura petroleira, nin é un estaleiro indicado para a renovación da frota menor de Pemex. Por iso, Pemex xa negociaba con varios outros estaleiros galegos sobre a frota menor e sobre outro flotel. Entón, Barreras xestionará negocios navais con Pemex para todo o 'ecosistema' de estaleiros galegos? Será positivo que esa adquisición poda 'crear capacidade construtora de buques especializados en México', como promete Pemex. Que nos expliquen como".

Ademais, o analista apunta a unha artimaña do Goberno mexicano e Pemex para saltarse a legalidade na compra de Barreras, dándolle a volta ao Artigo 134 da Constitución mexicana, que "obriga a concursar as adquisicións públicas en México. (Recorden que PMI Internacional, o brazo comercial de Pemex, asumiu e firmou o compromiso de construír os floteis, para ofrecelos directamente a PEP)", advirte Shields, quen conclúe: "Vese difícil que Pemex poda encargar obra pública mexicana futura sen licitación a ese estaleiro, agás que sexa a través dun arranxo coa Secretaría de Marina para renovar a frota menor".

Finalmente, David Shileds cuestiona o acordo ao considerar que "hai problemas de opacidade e ética non resoltos neste asunto".

"Ademais, a situación laboral e social é tensa e conflitiva nos estaleiros galegos, reflexando a severa crise económica española. Esa lea tamén a compraría Pemex? É moi loábel que México e Pemex queran apoiar a España, pero nos convén así ese negocio?", pregúntase.

Tamén o xornal mexicano La Jornada cuestiona nun editorial o contrato entre Pemex e Barreras, "subscrito practicamente en secreto e sen licitacións públicas de por medio", e advirte de que "a discrecionalidade nestes asuntos pode resultar moi custosa, como quedou de manifesto coa aventura corporativa de Pemex en Repsol, e non só en termos de perdas económicas, senón tamén en desgaste da credibilidade da administración pública no seu conxunto".

Estratexia fallida e polémica en Repsol

Pemex ten experiencia en España como inversor desde o ano 1979, cando fixo investimentos en Petróleos do Norte, S.A. (Petronor) —hoxe filial de Repsol—, do que se converteu no primeiro accionista cunha participación do 34.28 %. No ano 1990 acordou co Instituto Nacional de Industria (INI) o troco da súa participación en Petronor por accións de Repsol, de cuxo grupo é socio fundador, e pasou a converterse nun dos seus maiores accionistas. Pemex autocualificouse como "socio leal" de ambas as dúas sociedades.

Mais a súa experiencia non convida a ser optimista de cara ao futuro de Barreras. O 29 de agosto de 2011, Pemex acordou co conglomerado construtor español Sacyr-Vallehermoso votar conxuntamente como accionistas de Repsol para facerse co control da compañía. Os pequenos inversores da petroleira española denunciaron entón que ese acordo carecía de transparencia e acusábanos de incumprimentos legais e uso de información privilexiada. A paraestatal mexicana defendeu ante a Comisión Nacional del Mercado de Valores española (CNMV) a legalidade da súa operación.

A Asociación Española de Accionistas Minoritarios de Empresas Cotizadas (Aemec) solicitara á CNMV indagar se Pemex usara información privilexiada na compra do 4,69% de Repsol, porcentaxe que sumada ao 4.8% que xa controlaba, alcanzaba o 9,4%, converténdose no terceiro accionista da compañía española, tras Sacyr-Vallehermoso e La Caixa catalana. Desde esa nova posición de poder, Pemex acordara sumar os seus votos no consello de administración aos da construtora, co 20 por cento das accións, formando así unha alianza de enorme poder na petroleira española. A operación para Pemex supúxolle un custo duns 600 millóns de dólares.

Na súa denuncia, Aemec consideraba que Pemex infrinxira a normativa de información privilexiada, abuso de mercado e de comunicación de informacións sospeitosas, así como a posíbel existencia dun cambio na estrutura de control de Repsol que obrigaría a presentar unha Oferta Pública de Accións (OPA) pola totalidade do capital social.

Como no caso de Barreras, Pemex pretendía utilizar tamén a tecnoloxía de Repsol para aumentar o seu programa de perforación mar adentro. A analista de Stratfor Karen Hooper xa advertía en 2011, nun correo intercambiado o 6 de outubro con colegas da axencia de intelixencia global, que tiña "claro" que esa era a intención principal de Pemex, que "non dispón da tecnoloxía para ampliar as reservas probadas, a produción e as reservas coñecidas están caendo, e o orzamento do Goberno depende en grande medida dos ingresos do petróleo para os seus gastos".

O aumento na participación no capital da española Repsol YPF foi o inicio dunha nova estratexia de expansión de operacións de Pemex no estranxeiro, que incluía, entre outros obxectivos, ampliar as súas exportacións de petróleo cru a novos mercados como India e China.

No ano 2011, o medio mexicano La Jornada revelou a estratexia global de Pemex, contida no documento 'Contexto do aumento de participación de Pemex en Repsol', no que se destacaba que a maior participación de Pemex en Repsol formaba parte dos plans estratéxicos de crecemento que a paraestatal mexicana trazara para incrementar a súa produción e incorporar novas reservas petroleiras. Estes obxectivos estratéxicos eran: adquisición e construción de activos internacionais que faciliten a loxística de produtos e, en particular, capacidade de procesamento, ductos e capacidade de almacenamento.

O que máis lle interesaba a Pemex era ter acceso a un amplo portafolio tecnolóxico de Repsol. O que buscaba a empresa mexicana era o acceso á tecnoloxía a un prezo moito máis barato do que lle custaría noutra compañía. A empresa mexicana quería conseguir como fose o programa de interpretación de datos de sísmica denominado 'Caleidoscopio', creado en 2007, que procesaba 15 veces máis rápido as imaxes que calqueroutra alternativa tecnolóxica. Este programa fora desenvolvido en colaboración coa Universidade de Stanford, IBM e o Centro de Supercomputadora de Barcelona (UPC). Co acceso a 'Caleidoscopio', Pemex podería utilizar estas ferramentas na exploración de augas profundas e nos campos de alta complexidade como Chicontepec.

Pemex tamén tiña interese en acceder a ferramentas como 'Sherlock', proxecto multidisciplinario de xeoloxía, xeoquímica e química analítica de alta resolución, que permitiría á paraestatal mexicana diminuír o risco xeolóxico e aumentar a taxa de éxito exploratorio.

Ao mesmo tempo, estaba buscando ter acceso a fontes adicionais de reservas e produción de xeito directo ou a través de alianzas para proxectos internacionais; por exemplo, en Cuba ou Brasil, onde Repsol posúe importantes portafolios de exploración.

Pemex negou que quixera roubarlle tecnoloxía a Repsol

O por entón director xeral de Petróleos Mexicanos, Juan José Suárez Coppel, asegurou que o obxectivo primordial ao ampliar o paquete accionarial en Repsol era ter un maior peso da paraestatal mexicana na toma de decisións da petroleira española, sen pretender o seu control.

Nunha entrevista con Carmen Aristegui, en MVS Noticias, Suárez Coppel rexeitou as acusacións de que a compra das accións de Repsol fose abusiva e negou que o seu propósito fose roubar tecnoloxía, principalmente a desenvolvida para a exploración en augas profundas.

O 2 de setembro, Pemex anunciou á Comisión Nacional do Mercado de Valores a compra do 4,69 por cento do capital de Repsol YPF, porcentaxe que se sumaba ao 4,8 por cento que xa controlaba desde 2008, despois de subscribir e renovar a súa participación en Repsol a través de *swaps* con institucións financeiras sobre 58 millóns 679 mil 799 accións polas que obtivo os dereitos económicos e de voto adicionais.

Nun comunicado enviado á CNMV, a empresa facía pública unha adquisición feita a través da súa filial nas Antillas Holandesas, P.M.I. Holdings, de 56 millóns 377 mil 90 accións de Repsol YPF por uns 1.150 millóns de euros.

Malia as declaracións do director de Pemex, en Repsol viron a operación como unha ameaza e decidiuse suspender os seus dereitos de voto e restrinxir a participación da paraestatal mexicana no consello de administración. O enfrontamento entre os accionistas mexicanos e españois derivou en accións legais e Pemex impugnou aquela decisión. Para os españois, era evidente que a paraestatal mexicana tiña un conflito de intereses por ser un competidor directo, especialmente na área de exploración, polo que a compañía mexicana podería verse obrigada a saír do consello.

Nun coreo entre analistas de Stratfor enviado o 28 de setembro de 2011, Robert Inks entendía que a intención de Pemex e Sacyr era "reestruturar" Repsol. Ademais, incidía tamén en que Pemex planexaba "utilizar o seu investimento en Repsol para obter acceso ás tecnoloxías de perforación en aguas profundas" da empresa española.

O plan pasaba pola "incorporación de Repsol á estrutura enerxética nacional" mexicana, apuntaba Inks, quen explicaba entón que "tal esquema, se ten éxito, podería ter un impacto significativo e positivo no futuro do petróleo de México".

Perdas millonarias e desinvestimento

Agora, logo de 20 meses e un investimento de 1.500 millóns de euros, Petróleos Mexicanos clasificou a súa participación accionarial de case o 10% na propiedade de Repsol como activos dispoñíbeis para a súa venda. A súa intención de desinvestir na petroleira española coincide coa súa toma de control do estaleiro galego Barreras, onde Pemex ten tamén como obxectivo prioritario a transferencia tecnolóxica cun custo moi baixo para os mexicanos.

Segundo a propia prensa azteca, os informes oficiais precisan que Pemex acumula xa unha perda dun 650 millóns de euros (equivalente a case o 50% do valor inicial da operación), pola adquisición, en agosto de 2011, de 57.204.240 accións, co que Pemex incrementou o dereito económico e de voto en Repsol até case o 10%. Unha operación que fora financiada no 70% coa contratación de débeda e o resto con recursos propios que mantiña a paraestatal en caixa.

A compra das accións de Repsol por parte de Pemex en 2011 realizouse a través de operacións con diversas entidades, entre as que se atopan HSBC, Credit Agricole CIB, Natixis e Grupo Financeiro Inbursa. O asesor financeiro desta transacción foi Credit Agricole CIB.

O entón director xeral de Pemex xustificou a compra de accións de Repsol non só polas ganancias financeiras que estimaba que lles reportarían, senón tamén por gañar en ideas, tecnoloxía, capacidade de execución e de xestión.

Na segunda quincena de abril de 2012, as accións de Repsol, en declive nos mercados financeiros internacionais, sufriron un gran descalabro despois de que a presidenta de Arxentina, Cristina Fernández de Kirchner, determinara nacionalizar o 51% das accións pertencentes a Repsol YPF, unha das filialis de máis valor da petroleira española.

Máis adiante, ante a imposibilidade de pagar utilidades en efectivo, o 19 de xuño de 2012 Repsol emitiu un programa de pago de dividendos en accións, polo que o 5 de xullo de 2012 Pemex recibiu 2.600.191 accións como pago de dividendos en especie.

Ao peche do primeiro trimestre de 2013, e segundo o valor de mercado das 59 millóns 804 mil 431 accións, Pemex arrastra unha perda duns 643 millóns de euros.

Desconfianza

Mentres Pemex fala de afastarse de Repsol, o presidente da compañía española ofrece unha versión radicalmente oposta e di que é a petroleira española a que non quere a Pemex no seu accionariado.

As fontes de Repsol aseguran que o seu presidente, Antonio Brufau, "non se fía dos mexicanos" tras os seus movementos con Sacyr.

Tampouco a prensa mexicana se fía xa das operacións da paraestatal do seu país e xornais como La Jornada cualifican de "fracaso rotundo" a aventura de Pemex en Repsol.

"Agora, Pemex se apresta a pechar un novo negocio coa adquisición dun estaleiro en creba en Vigo, España", di en ton de desconfianza a prensa mexicana.

Problemas financeiros e "incompetencia" na xestión

O peso de Pemex é de vital importancia para as arcas do Estado mexicano. A empresa paraestatal viu aportando o 80% dos seus ingresos ao Goberno daquel país, que cubren aproximadamente o 35%-40% dos orzamentos nacionais, pero a súa produción e exportacións se resentiron nos últimos tempos e isto puxo en alerta a Administración federal. De feito, Pemex ten problemas de liquidez e a súa débeda é descomunal.

No ano 2008, os expertos xa advertiron de que "agás que Pemex aumentase a súa produción de petróleo", o país debería "enfrontarse a un enorme buraco no seu orzamento". De feito, as cifras de produción da paraestatal ofrecían unha "lectura alarmante" pola súa caída, segundo un informe publicado en LatinNews.

Nesta análise, "os enxeñeiros do petróleo" amosábanse "atordados pola magnitude da caída". Non en van, "as compañías petroleiras internacionais calculan que se a produción dun campo petroleiro cae en máis dun 14% nun ano, algo está seriamente mal". E só na primeira metade de 2008 a produción de Pemex xa era un 9,8% menor que no mesmo período de 2007, a 2.85m de bpd [bpd=barrís por día]. E, "o máis alarmante", a produción dos xacementos petrolíferos máis importante do país durante as tres últimas décadas, o Complexo Cantarell, diminuíra un 28,4% en comparación co primeiro semestre de 2007, a un promedio de só 1.14m de bpd no primeiro semestre de 2008, explicaban os analistas, que advertían de que "calquera das cifras de produción anteriores ou ben foran esaxeradas ou a xestión das reservas do xacemento era de incompetentes".

Os analistas estaban vendo que "os efectos financeiros do colapso na produción de Pemex foron escurecidos polo aumento no prezo internacional do petróleo, que mantivo o fluxo de diñeiro". "O preocupante das políticas do Goberno mexicano", explicaban os expertos, era que "o volume de petróleo que Pemex exportara no primeiro semestre de 2008 era un 15,4% menor respecto ao mesmo período de 2007, a 1,45 m de bpd". E isto estaba "moi por debaixo do que o Goberno pesupostara para as exportacións de Pemex en 2008", que "tiña calculadas en 1.68m de bpd de media".

Nesta análise salientábase que o problema de Pemex era que fora "muxida dun xeito basto por unha sucesión de gobernos que substraeron o efectivo e lle obrigaron a pedir prestados cartos para financiar os seus investimentos".

A falta de investimentos gubernamentais na paraestatal fixo que "a capacidade de refinar de Pemex se limitase tanto que o 40% do combustíbel de México acabou sendo importado".

Un artigo publicado en The Economist en 2008 xa avisaba tamén de que "Pemex estaba acostumada a ser a vítima da mala concertación" e destacaba o "declive" da paraestatal: "Dende 2005, a produción diaria caeu en máis de 300.000 barrís por día, un 10% do total. As reservas estiveron caendo desde mediados dos anos oitenta".

O diario económico tamén incidía en que Pemex era vítima do "dispendio". "México ten que importar máis do 40% do petróleo debido á falta de capacidade de refinación. Logo, revéndese a prezos subvencionados á poboación. Gástanse un 20 millóns de dólares se no ano", explicábase.

Hai que recordar que a Constitución de México establece que a industria petroleira debe permanecer baixo o control do Estado, de aí que as suxerencias de permitir maior participación privada teñan provocado fortes reaccións en contra.

Paradoxalmente, malia ter a maior petroleira de América Latina, as facturas a pagar polo Estado mexicano polas importacións de combustíbel aumentaron. Así, "no primeiro semestre de 2008, México importou un promedio de 331.000 barrís diarios de combustíbel, fronte aos 294.000 bpd no mesmo período de 2007. O aumento do volume das importacións ocultaron os efectos monetarios: o custo das importacións de petróleo aumentaron un 54% entre o primeiro semestre de 2007 e o primeiro semestre de 2008".

Porén, e "para ser xustos", os analistas aclaraban que Pemex seguía sendo un "importante exportador de petróleo cru". Os seus ingresos por exportacións no primeiro semestre de 2008 foran de 24.800 millóns de dólares, é dicir, "un 52% máis que no mesmo período de 2007".

Perda de peso no mercado internacional

Con todo, México foi perdendo posicións nos últimos anos entre os maiores produtores de petróleo. No ano 2008 era o sexto produtor, segundo datos da Administración de Información de Enerxía de Estados Unidos. En 2012 xa baixara ao oitavo posto froito dunha caída incesante na súa produción dende o ano 2004, cando era o quinto produtor mundial, e pola "decadencia das súas reservas", segundo veñen observando os analistas, especialmente no xacemento de Cantarell, que viña aportando o 60% do total das extraccións.

O 28 de xuño de 2009, a analista de Stratfor Leticia Pursel xa prognosticaba nun correo interno da axencia de intelixencia global que "a seguridade enerxética" se convertiría "nunha das ameazas máis importantes para a seguridade nacional de México nos próximos cinco a dez anos".

"A caída na produción de petróleo cru, os prezos do petróleo internacionais e a dependencia de Pemex nos ingresos fiscais, son ameazas graves para México", sentenciaba a analista nunha comunicación co analista de xeoestratexia Marko Papic.

Pursel foi aínda máis contundente ao criticar a actuación da política mexicana respecto a Pemex: "A reforma petroleira recentemente aprobada polo Congreso mexicano reflexa a pouca visión das autoridades mexicanas sobre o papel xeopolítico e estratéxico que México debe ter no continente".

A analista sinalaba tres "limitacións" fundamentais: "1) a restrición do capital privado nas actividades de petróleo e gas; 2) o uso de case 10.000 millóns de dólares para a construción dunha refinería en México (malia que Estados Unidos ten case 150 e Canadá 50), cando ese diñeiro debería ser utilizado mellor no investimento en ciencia, tecnoloxía e investigación co fin de aumentar a produción; e 3) a súa posicióncontra a proposta norteamericana de integración rexional entre os tres países, que inclúe a seguridade enerxética".

Leticia Pursel considerou este asunto como "unha das enormes ameazas que México enfrentorá na próxima década".

Nun correo enviado o 27 de decembro de 2010 polo analista económico Robert Reinfrank á estratega experta en América Latina Reva Bhalla, ambos os dous tamén da axencia intelixencia global Stratfor, destacaba que o problema clave para Pemex non era tanto o roubo de cru en cantidades inxentes por parte das redes de narcotraficantes, como o "declive da produción nacional debido ao seu difícil clima de investimento". Neste sentido, sinalaban que "a prohibición constitucional aos investimentos estranxeiros nos recursos naturais de México levaron a un baixo investimento nas industrias extractivas".

Ese mesmo ano, a axencia Stratfor realizaba o informe 'Mexico: Business-Risk Assessment', unha avaliación de riscos para o país no que se avisaba de que "as medidas a medias" postas en marcha para reformar o sector enerxético mexicano "farán pouco para revertir a diminución do sector enerxético e proporcionar maior financiamento para o Estado".

Outro informe de Stratfor, de febreiro de 2011, salientaba o declive de Pemex, que perdera 4.740 millóns de euros en 2010, é dicir, un 80,4% máis que en 2009. Segundo os analistas desta axencia, dúas razóns explicaban as perdas: "os impostos onerosos e a diminución da produción no seu principal campo, o de Cantarell".

En maio dese mesmo ano, a Organisation for Economic Co-operation and Development (OECD) publicaba outro informe no que prognosticaba que México necesitaba unha reforma do sector enerxético "para evitar a dependencia dos orzamentos do Goberno dos ingresos do petróleo e da súa volatilidade", e apuntaba a que só para manter os actuais niveis de produción de petróleo mexicano, estábel nos últimos anos, pero moi por debaixo dos anos de ouro de Pemex, a paraestatal está obrigada nos próximos dez anos a facer "importantes investimentos continuos" que suporán "altos custos de exploración e novos descubrimentos" que poderían incrementar a enorme débeda que xa arrastra a empresa parestatal.

A produción de petróleo mexicano caeu de xeito significativo nos últimos anos, como se observa no seguinte gráfico.

O certo é que o declive é evidente e o discurso oficial mexicano sobre unha recuperación da produción e comercialización de petróleo nos próximos anos foi comprometido polos cables aos que tivo acceso WikiLeaks, nos que o ex-embaixador de Estados Unidos en México, Carlos Pascual, recoñecía en 2010 que, contra os prognósticos optimistas do Goberno mexicano, non hai opcións realistas para revertir esta diminución no curto ou medio prazo.

Por outro lado, Dave Graham publicaba en agosto de 2011 na axencia Reuters un artigo no que cuestionaba o gasto de miles de millóns de euros de Pemex no seu proxecto Chicontepec, e cuxos resultados "están moi por debaixo das expectativas".

A estes problemas engadía "a inseguridade derivada de guerra contra o narcotráfico" e os "roubos de petróleo e gas por valor de case o 70 por cento das súas ganancias" só no primeiro trimestre dese ano.

Noutro correo de Stratfor enviado o 31 de maio de 2011, a analista Karen Hooper explicaba que a "falta de investimentos e a diminución da produción causaron unha caída na saída de petróleo dun 22 por cento entre os anos 2004 e 2010".

Hooper consideraba que as reformas postas en marcha no ano 2008 para abrir a Pemex a investimentos foráneos "carecían das medidas necesarias para fomentar a entrada de capital estranxeiro e tecnoloxía na industria e non puido facer fronte ás principais debilidades institucionais que permiten a corrupción masiva e as malas prácticas comerciais en Pemex".

"Cos ingresos do Goberno altamente dependentes do desempeño de Pemex, é urxente que México resolva o problema da diminución da produción", advertía xa a analista de Stratfor.

Máis duros teñen sido os analistas mexicanos. Nun editorial de La Jornada publicado o 19 de marzo de 2012, o xornal acusou á Secretaría de Facenda e Crédito Público mexicana de "saqueo fiscal" de Pemex e denunciaba a "opacidade extrema no manexo das súas finanzas e na relación cosindicato", ademais de no "contratismo con particulares". La Jornada tamén falaba de "sobrexplotación a todas luces desaconsellábel e perigosa, coa pretensión de levar a produción a promedios diarios de tres millóns de barrís de cru". Todo este "cúmulo de vicios" que vén arrastrando a paraestatal mexicana contribuíron de xeito decisivo a comprometer a súa viabilidade financeira. De feito, para La Jornada, é máis que evidente o "debilitamento e erosión da paraestatal".

Irregularidades nas contratacións

Os xestores de Pemex movéronse tradicionalmente no secretismo e a opacidade. A presunta irregularidade na adquisición de Barreras, saltándose a legalidade, non é nada novo. Por exemplo, Alejandro del Río denunciaba o 5 de agosto de 2011 en Tabasco Hoy, o maior xornal deste Estado, que as contratacións doutras empresas por parte de Pemex non se estaban realizando pola vía da licitación, como era de esperar. O xornal era duro no titular: "I.I.I. Servicios, brazo impune de Pemex".

O diario insinuou que "a constitución de I.I.I. Servicos, S.A. de C.V. tiña o fin de evitar os molestos e longos procedementos de licitación para as contratacións en Petróleos Mexicanos, ou ben, ser a empresa que fomentará a participación das PeMES na industria petroleira".

"O certo é que o negocio, xunto coa Compañía Mexicana de Exploraciones (COMESA) estanse convertendo nunha forma de legalizar a entrega de contratos sen que se fagan pola vía da licitación", denunciaba o xornal.

O diario tabasqueño recordaba que a empresa I.I.I. Servicos estaba "sinalada como a principal responsábel —xunto ás empresas Gutsa Infraestructura/ Proyectos y Desarrollos de Infraestructura SAPI— polo fracaso e o encarecemento da construción 'Ronsel de Luz', que debeu quedar construída a finais do ano 2010; porén, non foi así", denunciaban.

O obxecto social desta filial era prestar e realizar os servizos de administración e operación a Instalacións Inmobiliarias para Industrias e a Petróleos Mexicanos, e os seus Organismos Subsidiarios. O que se descubriu foi "unha cloaca como outra vía para legalizar e fomentar a corrupción á hora de contratar obras e servizos dentro da industria petroleira, tal e como ocorre en COMESA", acusaba o xornal.

Do total de 1.271 obras e servizos entregadas pola empresa desde o ano 2006 deica o 14 de xullo de 2011, 858 foron por adxudicación directa, 66 por invitación a polo menos tres persoas e o resto, 347, por licitación pública nacional, segundo datos do Portal de Obligaciones de Transparencia do Goberno mexicano. "É dicir, I.I.I. Servicos impediu a participación de centos de contratistas polo simple feito de adxudicar directamente 858 obras que por monto deberon ser concursadas", publicaba Tabasco Hoy.

"Se non é por tráfico de influencia ou corrupción, de que outro xeito podería entenderse que, por exemplo, unha empresa como MAJA Consulting Group, sen ningún tipo de experiencia, lle adxudiquen directamente os contratos I I I S - C OP - SOP-099-10, por un monto de 93 millóns 379 mil 576,12 pesos; IIIS-COM-SOP-100-10, por 64 millóns 899 mil 356,14 pesos; IIIS-COM-SOP-118-09, por 18 millóns 300 mil 163,58 pesos; e o IIIS-COM-SOP-105-09 por 14 millóns 880 mil pesos?", preguntábase Alejandro del Río, quen ofrecía máis exemplos de presunta corrupción.

Hai documentados máis casos de irregularidades nas contratacións de Pemex. Por exemplo, a adxudicación presuntamente irregular dun contrato de asesoría e mantemento por 42 millóns de dólares á empresa estadunidense KBC Advanced Technologies Inc., denunciada polos lexisladores da Comisión de Enerxía da Cámara de Deputados ante a Secretaría da Función Pública e a Contraloría Interna de Pemex, en agosto de 2011.

O xornal Milenio informaba de que fora o subdirector de Pemex Produción e Refinación, Bernardo de la Garza Hesles, "quen asignou directamente o contrato, por enriba do seu xefe inmediato, Miguel Tame Domínguez, director da subsidiaria".

Que futuro lle agarda a Barreras?

Se o analista David Shields cuestiona a conveniencia para Pemex de facerse cunha empresa en creba como Barreras, nun contexto ademais de crisie económica e conflitividade social como o que vive España, desde aquí cabe cando menos cuestionar tamén a incursión de Pemex no naval galego e resolver as dúbidas e incertezas que xenera un acordo cunha empresa, a mexicana, en creba técnica e intervida pola corrupción, as bandas criminais, as irregularidades, a opacidade, a incompetencia dos seus xestores e intereses partidistas. E con todo, a pregunta vital agora é: levará a cabo Pemex a transferencia tecnolóxica completa para trasladar o estaleiro vigués a México nun medio prazo?

Estación de Pemex | Fonte: *Travis S. en Flickr*

ANEXO XIX: Publicación 11 de los correos de Stratfor.

Pemex (III): a 'caixa chica' de políticos e paraíso de sindicalistas corruptos

Terceira e última achega da serie de artigos de análise sobre o novo dono de Barreras. Petróleos Mexicanos é considerado a "caixa chica" de políticos daquel país. O seu sindicato recibe ademais millóns de euros para dispendios, impón a contratación dos seus traballadores a navieiras privadas e o seu secretario xeral é acusado de nepotismo.

- Pemex (I): corrupción, crimes e inseguridade no novo dono de Barreras
- Agora en aberto: Pemex (II): opacidade, creba técnica e deslocalización de Barreras
- Axudar ao GC é agora máis doado e rápido

Por Alberto Quian | Vigo | 20/05/2013 | Actualizada ás 08:00

Pemex, fundada en 1938, é a maior empresa de México e a petroleira máis grande de América Latina. Está controlada polo Estado mexicano baixo un réxime constitucional e é símbolo do nacionalismo mexicano e do paternalismo do Estado, polo que calquera mínima insinuación ou idea de privatizar a paraestatal sempre xenerou controversia no país azteca. Só hai que recordar as palabras do anterior presidente mexicano, Felipe Calderón Hinojosa, para entender o simbolismo da paraestatal: "Quero deixar claro que o petróleo é e seguirá sendo propiedade exclusiva de México. Pemex non se privatiza. O petróleo é un símbolo da soberanía da nación".

Asteleiros Barreras, que pasarán a mans de Pémex | Fonte: *economiadigital.com*

Porén, en documentos publicados por WikiLeaks en 2012 descubriuse que o Goberno mexicano estivera negociando en segredo abrir as portas de Pemex a compañías internacionais, segundo afirmacións de Georgina Kessel –a primeira secretaria de Enerxía do goberno do presidente Felipe Calderón Hinojosa– ao exembajador de Estados Unidos en México Carlos Pascual, recollidas polo propio diplomático nun despacho ao Departamento de Estado de Estados Unidos. Os documentos revelados por WikiLeaks poñían ao descuberto que o goberno de Felipe Calderón mantivera un dobre discurso, un en público radicalmente oposto ao negociado nas reunións privadas coa súa contraparte.

A industria petroleira mexicana está dominada por Pemex, que ten o monopolio absoluto sobre a exploración e produción de petróleo e gas nacionais, así como a refinación e comercialización de petróleo e produtos derivados deste. Hoxe, México é o oitavo produtor de petróleo do mundo; porén, este país foi perdendo posicións nos últimos anos pola caída incesante na súa produción dende o ano 2004, cando ocupaba o quinto posto mundial, e pola decadencia das súas reservas.

Ademais, as aportacións da paraestatal aos orzamentos do Estado son fundamentais para a economía mexicana, xa que representan entre o 35% e o 40% dos orzamentos estatais, e das súas caixas saíron inxentes cantidades para financiar campañas presidenciais.

Por todo isto, Pemex foi obxectivo prioritario nos últimos anos dos *cárteles* da droga, ademais de ter inoculada a corrupción na súa estrutura, dende a súa base laboral até altos cargos.

Torre Pemex, sede central da empresa paraestatal mexicana | Fonte: *Eneas*

Mais a pronunciada caída da súa produción, a ineficiencia do seus xestores, as perdas millonarias e unha descomunal débeda de 48.000 millóns de euros puxeron a Pemex nunha situación de creba técnica que compromete o futuro inmediato da paraestatal.

O control político

Creada despois de que o presidente Lázaro Cárdenas nacionalizara a industria mexicana do petróleo no ano 1938, as aportacións de Pemex á Administración mexicana representan entre o 35% e o 40% dos seus orzamentos anuais.

A compañía foi tratada como unha galiña de ovos de ouro polos sucesivos gobernos, pero especialmente durante os 71 anos de goberno ininterrompido do PRI, que chegou mesmo a canalizar decenas de millóns de euros en fondos de Pemex para a súa fallida campaña presidencial do ano 2000.
A decadencia de Pemex levou aos seus xestores e á clase política que domina este imperio petroleiro a replantexar a súa estratexia de cara a súa supervivencia as próximas décadas, da que depende non só a economía mexicana, senón tamén os dispendios políticos e sindicalistas.

Na segunda metade de 2011, a paraestatal iniciou un cauto proceso histórico de apertura a empresas privadas coa asignación dos primeiros contratos de exploración e produción de petróleo. Deste xeito, o Estado mexicano buscou elevar os seus debilitados niveis de produción. Así, Pemex foi recollendo os primeiros froitos da leve reforma enerxética aprobada en 2008 polo Congreso mexicano que lle permite á paraestatal flexibilizar a súa estrutura de contratacion sen por iso deixar de estar en mans do Estado. Con todo, isto fixo aflorar de novo os sentimentos nacionalistas. Por exemplo, a secretaria da Comisión de Enerxía mexicana, a deputada Laura Itzel Castelo Juárez, asegurou que os contratos que outorgara Petróleos Mexicanos a empresas privadas en campos petroleiros de Tabasco "violentaban" a Constitución e representaban unha "regresion para o crecemento do país".

GC tivo acceso a un correo do 22 de setembro de 2011 entre membros da axencia de intelixencia global Stratfor, no que o seu analista Benjamin Preisler remitía as consideracións das súas fontes en México. Estas describían a Pemex como unha empresa que está absolutamente dominada pola Secretaría de Facenda do país azteca. Stratfor buscaba coñecer máis a fondo as relacións entre as cúpulas de Pemex e as do Partido Revolucionario Institucional (PRI) e do Partido Acción Nacional (PAN). No correo adiantábanse algunhas das claves da nova estratexia da paraestatal:

> "É moi importante que teña en conta a importancia económica de Pemex. O 35% dos ingresos fiscais do Goberno mexicano veñen de Pemex. Isto significa que o grupo de control de Pemex sempre é o da Secretaria de Facenda. Asi foi en tempos do PRI e segue sendo en tempos do PAN. As grandes decisións veñen de Facenda ou teñen que ser aprobadas por Facenda. A xustificacion é que é prioritario non poñer en risco as finanzas públicas. Sendo un ente tan complexo, o tema non se esgota aí. O sindicato, que ocupa cinco lugares no consello de administracion, é *priísta*. Ten unha relacion de colaboracion-confrontacion coa administracion. Colabora porque lle interesa que Pemex xere ingresos que lle permitan seguir muxindo a vaca. Confronta porque a súa vision de Pemex se opón a calquera intento de apertura ao sector privado da empresa. O PAN ten a posibilidade de colocar algúns cargos importantes no persoal administrativo non sindicalizado. Son propostos polo presidente e, en teoría, deberian cumprir un perfil técnico-administrativo, pero iso non ocorre sempre. Nun ano electoral (2012), é posíbel que os funcionarios de confianza actúen máis como *panistas* que como funcionarios profesionais. As reformas a Pemex non se intentarán en 2012. O escenario electoral fará que a axenda lexislativa sexa moi conservadora. Ninguén abordará temas polémicos. O director Suárez Coppel, que ten visión empresarial, tentará facer cousas que estean dentro do marco do permitido. Quizá vexamos outra operacion audaz, como a de Repsol. Sobre as reservas, as versións informais de Pemex dinnos o contrario. Hai descubrimentos interesantes que poderían levar as reservas probadas e probábeis a niveis mellores dos que se tiñan ao comezar o sexenio, en 2006".

Non ía desacertado o analista nas súas previsións, xa que Pemex concretou a finais de 2012 e inicios de 2013 talvez a súa operación máis audaz: facerse co 51% da maior factoría naval privada de Galicia por un prezo irrisorio: Hijos de J. Barreras.

Uns meses antes, en marzo de 2011, a analista de Stratfor Araceli Santos remitía outro correo no que informaba dunhas declaracións do entón presidente mexicano para defender a xestión política de Pemex, zarrapicada pola corrupción. Durante a 73ª conmemoración do aniversario da expropiación da petroleira mexicana, o presidente Felipe Calderón declarara que Pemex "non é a 'caixa chica' de ninguén e non pertence a ningún goberno, partido político ou facción, senón ao ao pobo mexicano", informaba Santos, quen aportaba declaracións do ex-presidente mexicano: "Estámonos asegurando de que Pemex opera en conformidade coas normas internacionais de transparencia e rendición de contas, polo que non pode haber máis contas segredas, non máis caixas chicas nesta empresa que pertence a todos os mexicanos".

Parte dos documentos revelados por WikiLeaks sobre Pemex, datados entre marzo de 2006 e xullo de 2008, demostran que o entón responsábel das finanzas da paraestatal, Juan José Suárez Coppel, negociou en segredo unha reforma da petroleira para procurar a apertura ao investimento estranxeiro para que Pemex puidese traballar de xeito independente. A proposta detallada nos cables da diplomacia estadounidense advertían da substitución de secretarios pertencentes ao consello de Pemex por analistas e especialistas en enerxía e finanzas. Negociacións nas que tería a aprobación do Partido da Revolución Democrática (PRD), encabezado polo seu entón candidato presidencial Andrés Manuel López Obrador, para o ingreso de inversionistas estranxeiros na paraestatal para realizar traballos de exploración en augas profundas. O obxectivo era resarcir con capital estranxeiro a descomunal débeda da paraestatal.

Nun dos cables publicados por WikiLeaks detállase unha reunión a finais de agosto de 2007 entre o entón subsecretario de Facenda mexicano, Alejandro Werner, e o asistente do Departamento de Economía estadunidense, Daniel Sullivan, na que se falou de Shell, ExxonMobil, British Petroleum, Halliburton e Schlumberger como os posíbeis inversionistas estranxeiros en Pemex. Os cables recollían unhas declaracións de Felipe Calderón en 2008 nas que advertía que era "necesario o investimento estranxeiro para salvar a Pemex", ao que a Embaixada de Estados Unidos comentou que "malia o rescate que se logre acordar para Pemex, este non será suficiente".

Varios dos cables filtrados por WikiLeaks apuntaron á debilidade financeira de Pemex, derivada do seu alto endebedamento, o cal abriu a opción a explorar "novos métodos de contratación" con empresas privadas foráneas.

Un sindicato corrupto

O Sindicato de Trabajadores Petroleros de la República Mexicana (STPRM) é un brazo armado dos políticos. O seu secretario xeral, Carlos Antonio Romero Deschamps, é senador polo PRI e é acusado de corrupción e dispendios millonarios. "É un sindicato secuestrado, secuestrado por Carlos Antonio Romero Deschamps. Ese señor non foi elixido pola clase traballadora, foi imposto con fins partidistas, con fins políticos", vén denunciando nos últimos tempos Omar Toledo Aburto, disidente do sindicato.

O STPRM desenvólvese na opacidade. Así, por exemplo, en abril de 2011, a analista de Stratfor Araceli Santos avisaba á axencia de intelixencia global estadounidense de que Pemex estaba ofrecendo "cifras contraditorias sobre o número de traballadores sindicalizados inactivos".

"De acordo coa información publicada por Pemex en resposta a unha petición para a liberación da súa información, entre xaneiro de 2007 e maio de 2009, un total de 1.666 traballadores sindicalizados e 262 membros das tripulacións dos buques de Pemex se mantiveron inactivos. Porén, o membro do consello profesional de Pemex Fortunato Álvarez declarara anteriormente que case 5.000 dos 11.500 traballadores de Pemex inactivos identificados en 2006 aínda non foran asignados a ningunha actividade, incluíndo persoal da planta petroquímica e das tripulacións dos buques que xa non operaban. Mentres tanto, o director xeral de Pemex, Juan José Suárez Coppel, declarou que 2.200 traballadores permaneceron inactivos e o departamento de recursos humanos da compañía reduciu aínda máis estas cifras. Suárez Coppel explicou que a empresa e o sindicato de traballadores do petróleo están revisando este asunto caso por caso, co fin de determinar se deben ser reasignados, xubilados ou despedidos os traballadores inactivos", explicaba a analista.

En agosto de 2011, Araceli Santos tamén informaba á axencia Stratfor de que "os armadores estranxeiros son obrigados a contratar empregados de Pemex". Santos subliñaba que ao amparo da cláusula 203 do contrato colectivo de traballo, as navieiras privadas deben aceptar entre as súas filas a empregados de Pemex como parte das súas tripulacións. En virtude desta cláusula, "as empresas privadas teñen que contratar a membros do Sindicato de Trabajadores Petroleros de la República Mexicana en varios postos se queren traballar con Pemex. A tripulación requerida nun barco de subministro vai de 14 a 17 persoas e o sindicato de Pemex proporcionaría entre 8 e 12 destes. A petroleira rexeitou comentar por que se aplica esta cláusula", explicaba a analista de Stratfor, quen engadía: "Representantes das compañías navieiras que gardan anonimato criticaron esta regra e comentaron que isto é tan absurdo como se as escolas privadas se visen obrigadas a contratar a funcionarios do Sindicato Nacional de Trabajadores de la Educación" de México.

Pemex sempre evitou facer comentarios sobre a aplicación deste tipo de cláusulas. Pola súa banda, empresas navieiras que solicitaron o anonimato aseguraron á medios mexicanos que a obriga de contratar a persoal do sindicato petroleiro colócaas en desvantaxe porque descoñecen se estes traballadores cumpren coas certificacións necesarias para o labor que realizarán.

Festas, viaxes e dispendios

Recentemente, varios medios mexicanos denunciaron as festas millonarias que vén celebrando o sindicato petroleiro nos últimos anos. Só entre os anos 2006 e 2012, o Sindicato de Trabajadores Petroleros de la República Mexicana recibiu transferencias directas por uns 112 millóns de euros por parte de Pemex para sufragar, entre outros conceptos, as viaxes dos líderes sindicais e os festexos para conmemorar a expropiación petroleira e o desfile do 1 de maio, de acordo co estipulado nas cláusulas 251 e 251 bis do Contrato Colectivo de Traballo (CCT).

Este documentos foron obtidos polo xornal El Financiero e denunciados previamente por WikiLeaks. Nestes, desvélase que só para cubrir os gastos de viaxe de 68 membros do Comité Executivo Xeral do sindicato a paraestatal entregou nese período de tempo referido 11,34 millóns de euros.

A prensa mexicana denunciou que estes recursos —que actualmente ascenden a uns 169.000 euros mensuais— son entregados puntualmente por Pemex sen que os líderes sindicais teñan que xustificar o motivo ou destino deses cartos, tampouco comprobar os gastos nin dar conta das persoas que os realizan.

Entre 2006 e 2012 Pemex transferiu uns 15 millóns de euros ao sindicato petroleiro como "axuda" para a celebración de festexos como o anual que se celebra para conmemorar a expropiación petroleira ou para o desfile obreiro do 1 de maio, conmemoración esta última que non se celebra desde hai varios anos, malia o cal segue sendo sufragada.

Segundo El Financiero, "por concepto de gastos de contratación derivados das revisións anuais ao Contrato Colectivo de Traballo", Pemex entregou ao sindicato uns 44,5 millóns de euros desde o 1 de xaneiro de 2006 deica o 31 de decembro de 2012; unha cantidade por ano que a paraestatal transfire antes do inicio de cada revisión anual do Contrato Colectivo de Traballo e que nese tempo aumentou de 5,3 a 7,6 millóns de euros.

E baixo o concepto de "apoio económico directo ao Comité Executivo Xeneral" do sindicato petroleiro, Pemex entregou aos dirixentes sindicalistas uns 37 millóns de euros nese mesmo período.

A todas estas cantidades hai que sumar "o apoio económico para gastos de fomento para actividades deportivas e culturais" que vén aportando Pemex ao sindicato desde 2010, para as cales a empresa transferiu en tres anos ao sindicato uns 3,9 millóns de euros.

Millóns de cartos públicos dos que se descoñece en que ou como se utilizan por parte dos dirixentes sindicais.

Nepotismo no sindicato e vida de millonarios

Os sindicalistas de Pemex foron tradicionalmente os máis remisos á entrada de investimentos privados na paraestatal; non en van, os sindicalizados sempre gozaron de enormes privilexios e a súa cúpula vive a corpo de rei coma millonarios grazas á inxección que reciben de cartos públicos.

O caso máis chamativo e denunciado é o do fillo do líder sindical e senador *priísta* Carlos Romero Deschamps, quen vive a a todo luxo en Miami. José Carlos Romero Durán ten dous apartamentos en Miami Beach polos cales pagou 7,5 millóns de dólares, de acordo cos rexistros da propiedade. Un conta con 340 metros cadrados e foi comprado polo fillo de Romero Deschamps o 14 de decembro de 2005; o outro ten 530 metros e comprouno o 28 de marzo de 2006.

Ademais, Carlos Romero Deschamps regalou ao seu fillo un automóbil Enzo Ferrari, edición limitada do que só existen 399 unidades, valorado en preto de 2 millóns de dólares. Para poder comprar este modelo era necesario contar con cando menos dous Ferrari, demostrar solvencia económica, que o país onde vaia circular o vehículo conte cunha axencia automotriz da marca italiana, someterse a unha sofisticada proba de manexo e facer un só pago íntegro polo modelo.

A filla do do secretario xeral do sindicato, Paulina Romero, tamén vive entre o luxo e a opulencia: viaxes por todo o mundo en avións privados, comidas nos restaurantes máis exclusivos, noites nos hoteis máis caros, paseos en iates, as marcas de moda máis prestixiosas e luxosas...

Ademais, o diario Reforma denunciou que familiares de Carlos Romero Deschamps teñen contratos con Pemex que lles garanten traballo na paraestatal até o ano 2999 e reciben prestacións, malia que non traballan, e mesmo poden herdar eses postos a outros familiares.

O futuro de Barreras

O obxectivo que persegue Pemex, a través do vehículo de investimento seleccionado, é transferir a mediano prazo o coñecemento tecnolóxico de Hijos de J. Barreras para crear capacidade construtora de buques especializados en México e así poder atender a demanda de Pemex e modernizar a súa envellecida frota.

Para levar a cabo esa transferencia tecnolóxica, a paraestatal mexicana podería impor tamén a Barreras a contratación de empregados de Pemex no estaleiro vigués para formalos e levar a cabo os seus plans, o que reduciría dun xeito notable as expectativas de creación de emprego para os traballadores cualificados galegos. Ademais, ninguén desbota xa que esa transferencia tecnolóxica poda ser o paso para a deslocalización da empresa galega nun medio prazo e a estocada definitiva á industria navieira viguesa, se non se poñen en marcha estratexias que garantan a actividade dos estaleiros vigueses a longo prazo, unha vez que os mexicanos leven os recursos tecnolóxicos ao seu país.

Estación de Pemex | Fonte: *Travis S. en Flickr*

ANEXO XX: Entrevista a Richard Stallman.

"O nivel de vixilancia en Internet supera o que había na Unión Soviética"

Se pensa que os hackers son unha ameaza para a súa seguridade e para a de todos nós, talvez debería ler esta entrevista. Logo da súa xira polos campus universitarios de Vigo, A Coruña e Ourense, falamos con Richard Stallman, o hacker fundador e gurú do movemento mundial polo software libre, autor do termo copyleft —a antítese do copyright— e pai do proxecto GNU para o desenvolvemento dun sistema operativo libre completo.

Por Alberto Quian | Madrid | 18/12/2013 | Actualizada ás 08:00

Se cría que o hacking é cousa exclusiva de programadores informáticos, talvez debería escoitar e ler ao neoiorquino Richard Stallman, gurú mundial do software libre e un daqueles hackers do prestixioso e glorificado Massachusetts Institute of Technology (MIT) que nos anos setenta e principios dos oitenta fixeron evolucionar a un novo estadio a computación e o uso do software —a lóxica das computadoras—. Hoxe, ningún deses trebellos tecnolóxicos *intelixentes* que nos conectan co mundo, coa totalidade, estarían ao noso alcance de non ser polos hackers informáticos. Ás primeiras comunidades de hackers, as aparecidas nas décadas dos anos sesenta, setenta e oitenta en Estados Unidos, debémoslles esta revolución tecnolóxica que o toca todo.

Richard Stallman, durante a conferencia que ofreceu na Escola Superior de Enxeñaría Informática de Ourense | Fonte: *Duvi*

Libérese, pois, de prexuízos. Os medios tradicionais de masas mentíronlle sobre os hackers. Solte a carga semántica negativa que inocularon prensa, radio e televisión sobre a palabra hacker. Desbote interpretacións reducionistas sobre o hacking. Vostede pode ser un hacker. Créao ou non, así é. Só ten que empregar a súa intelixencia con espírito brincadeiro para resolver algo difícil, gozalo e recrearse nesa labor, sexa útil ou non. Non importa se é no mundo da informática, do xornalismo, da ciencia, da música, da poesía.. ou da vida cotiá. Explore os límites do posible con alegría. Estará hackeando. Non se confunda, os hackers hipermodernos non son os ciberdelincuentes que poden asaltar a súa vida pola porta traseira da súa computadora ou teléfono móbil. Os hackers hipermodernos son persoas como Lady Gaga... ou coma vostede talvez. Pensar e resolver como coller seis palillos chineses, tres en cada man, manipulalos individualmente sen que caiga ningún e coller unha porción de comida ten o valor dun hack, nada práctico, certo, pero gratificante se se fai con alegría. Palabra de gurú hacker, a de Richard Stallman, tamén coñecido como RMS ou St. iGNUcius.

A seguinte entrevista é un extracto dunha parola que mantiven con Stallman como parte do meu traballo para a miña tese doutoral en Investigación en Medios de Comunicación na Universidade Carlos III de Madrid.

- Qué é ser hacker?

- A palabra hacker ten varios significados diferentes. Para min é gozar do emprego da intelixencia cun espírito brincadeiro. Esta definición é o meu intento de buscar o que hai en común entre os varios usos que fixemos deste término. A palabra hacker empezouse a usar no MIT e noutras institucións relacionadas, por exemplo, a Universidade de Stanford, xa que había bastante migración de xente entre estas. Foron partes da mesma comunidade. O caso é que usabamos a palabra hacker de varias maneiras, pero o que tiñan en común era o uso da intelixencia cun espírito brincadeiro e non necesariamente na informática. O hack era posible noutras actividades tamén.

Richard Stallman, gurú mundial do software libre, na súa visita a Vigo | Fonte: *Duvi*

- Por que esa imaxe negativa que transmitiron dos hackers os medios de comunicación de masas?

- O que sucedeu foi que sobre os anos 1980-1981 os medios de comunicación se decataron da nosa existencia, pero fixérono con gran confusión porque só se fixaron nun aspecto limitado do hacking, nunha das actividades que algúns hackers facían ás veces, a de romper a seguridade informática para gañar acceso ás computadoras. E para gañar acceso facía falla usar a intelixencia cun espírito brincadeiro. Pero é incorrecto supor que ser hacker signifique só romper a seguridade. O único que se quería daquela era poder ter acceso e usar en calquera momento algunha computadora do MIT para a investigación... Non se fixo para danar nada e a ninguén, senón só para romper unha regra que bloqueaba o acceso. Non o considerabamos malo, non había por que facelo. Só foi algo malo para os autoritarios, para os que pensan en termos de obediencia. Porén, outros hackers pensaron máis alá. No laboratorio onde eu traballaba, o equipo de desenvolvemento do sistema operativo decidiu non introducir seguridade informática. Moito mellor que romper a seguridade das computadoras foi non ter seguridade para usar as computadoras sen obstáculos.

- Coa popularización de Internet, dos medios e redes sociais, e o desenvolvemento da sociedade rede, espallouse un novo fenómeno, o do hacktivismo, cunha dimensión política que talvez non tiña o hacking...

- Si, o hacktivismo ten unha dimensión máis política. Pero quero enfatizar que nós, os hackers, aínda insistimos en que hack significa moito máis que aquilo de romper a seguridade para o desenvolvemento informático. Por exemplo, Lady Gaga é hacker de roupa. O que fai coa súa roupa é empregar a súa intelixencia cun espírito brincadeiro. E se es hacker podes apreciala como hack. Porque ser hacker non só significa que che gusta empregar a túa intelixencia cun espírito brincadeiro, senón tamén probablemente que gozas vendo que outros o fan e como o fan, que desfrutas vendo os seus logros.

- Pero mudou o movemento hacker?

- Nunca foi un movemento. Non se trata dun movemento, senón dun gusto. Se tes o gusto da intelixencia brincadeira, se eu fago algo que demostra esa intelixencia, gustarache velo e tamén desexarás lograr tales cousas para amosar aos demais. É máis ou menos un tipo de arte.

- Aportaron algo as redes sociais aos hackers?

- Disto, das redes sociais, non sei nada. Só sei o que lin, porque non as uso.

- Por que?

- Non as uso porque, primeiro, sería incómodo para min e, segundo, porque nalgúns casos son abusivas cos usuarios, como por exemplo Facebook, que é un sistema para espiar a xente. Eu dígolle a todo o mundo que non poña as miñas fotos en Facebook.

- Pero semella que Internet e as redes socais ampliaron o impacto dos hackers na sociedade...

- Evidentemente, hoxe dise moito máis acerca dos hackers. Os medios de comunicación adoitan a usar o termo hacker para significar quen rompe a seguridade informática. Pero tamén vemos máis artigos hoxe en día cunha maior tendencia que hai dez anos a falar de hackers co significado de explorar os límites do posible en calquera campo técnico.

- Insiste en hackear como un acto para gozar. Pero, non ten o hacking unha dimensión ética, filosófica e política?

- Si, no campo do hacking pódense atopar as dimensións ética, filosófica e política.

- Na obra 'A ética do hacker e o espírito da era da información', o profesor Pekka Himanen falounos dunha nova moral que desafía a ética protestante do traballo que dominou a nosa cultura, especialmente dende a revolución industrial. Cre que se pode producir o cambio?

- Eu non falo de ética hacker, para min é simplemente gusto, un tipo de arte. É un poco como a poesía. Hai quen compón poemas e goza dos poemas doutros ao tempo que amosa orgullo dos poemas que compuxo. Hai unha actitude que vai coa práctica do hack igual que a que hai na poesía.

- Considérase parte dunha revolución social pola vía tecnolóxica?

- Eu non diría que se trate dunha revolución. Normalmente os hackers non desexan facer unha revolución. Ser hacker non implica ningún desexo de cambiar o mundo. Fundamentalmente é un desexo de lucir a túa intelixencia brincadeira, como sucede por exemplo co poeta cando compón poemas. No meu artigo 'On Hacking' cito como exemplo o palíndromo musical 'Ma Fin Est Mon Commencement' de Guillaume de Machaut, unha peza do século XIV que foi un bo hack.

- Que son para vostede Julian Assange, fundador de WikiLeaks, e Edward Snowden, o analista da NSA que descubriu ao mundo o sistema de espionaxe masivo da Axencia Nacional de Seguridade dos Estados Unidos?

- Son heroes.

- Heroes hackers?

- En WikiLeaks hai un aspecto de hack. No acto de Snowden non vexo tanto de hack, o seu é un acto político para actuar contra unha tiranía, pero non vin en Snowden o gusto do hack que si vin en WikiLeaks. Teño a impresión de que Assange gusta tamén deste aspecto da intelixencia brincadeira facendo o que fai.

- E os ciberactivistas de Anonymous?

- Eu non vexo esta actitude propia do hacker en Anonymous. É posible que alguns tivesen esa actitude, por exemplo no desenvolvemento dalgúns programas que usan. Pero a actitude xeral dos Anonymous non me parece que teña este espírito. En todo caso, é difícil afirmar calquera cousa respecto a todos os Anonymous. É posible que algún si o teña.

- Son cada vez máis as voces que alertan dos perigos en Internet baixo un sistema de vixilancia masiva por parte de gobernos e empresas que utilizan tecnoloxías da comunicación e da información para tal fin. Isto fai da Internet social unha utopía?

- Eu non sei que sería unha Internet social. Para min Internet pode ser un órgano de tiranía.

- Pensa que o está sendo?

- Estano facendo, evidentemente.

- Vostede fala da necesidade de limitar os niveis de vixilancia xeral na Rede. Superáronse os límites aceptables para unha sociedade democrática?

-Superáronse por moito. Vostede terá lido as denuncias de Snowden... Temos un nivel de vixilancia xeral moito maior que o que existía na Unión Soviética. Para ser compatible coa democracia habería que diminuír moito o nivel actual de vixilancia xeral.

- No centro do debate están as tensións que se producen entre o dereito á privacidade dos individuos e a vixilancia e secretos do Estado...

- Si. A loita é entre o secreto do Estado e a democracia. Os cidadáns non podemos ter o control do Estado sen saber que fai este. E para a democracia tamén fai falla o dereito á privacidade do individuo.

- E o software libre?

- Co software libre os usuarios teñen o control sobre o programa; co software privativo é o programa o que ten o control sobre os usuarios. Así que a loita polo uso de software libre tamén é fundamental para a democracia. Por iso penso que cada Estado debe recuperar a súa soberanía informártica cambiando o software privativo polo software libre.

- O software privativo que usan os Estados deixa a estes en mans doutras estruturas de poder?

- Exacto. O asunto é que co software privativo o programa ten o control do usuario e o dono do programa exerce o poder sobre este. E se o usuario é un Estado, o dono do programa exerce o poder sobre o Estado. Por iso o Estado ten que deixar de usar programas privativos.

- O escenario é orwelliano, o do totalitarismo do Gran Irmán...

- Si, así o creo. Por iso rexeito moitos produtos dixitais, o software privativo... Sabe, por exemplo, que Amazon borrou remotamente miles de copias dun libro aos usuarios de Kindle? Sabe que libro? '1984', de George Orwell. Isto simboliza o poder orwelliano que Amazon exerce sobre os usarios. Amazon é un produto orwelliano.

- E todo isto non se solucionaría pola vía lexislativa?

- Así é. Fai falla lexislar, porque nin as empresas nin os estados pararán de vixiarnos se non son forzados polas leis.

- Grazas.

- Happy hacking.

ANEXO XXI: Editorial de WikiLeaks publicado el 1 de septiembre de 2011.

Global - Guardian journalist negligently disclosed Cablegate passwords

1 September 2011

WIKILEAKS EDITORIAL

A Guardian journalist has negligently disclosed top secret WikiLeaks' decryption passwords to hundreds of thousands of unredacted unpublished US diplomatic cables.

Knowledge of the Guardian disclosure has spread privately over several months but reached critical mass last week. The unpublished WikiLeaks' material includes over 100,000 classified unredacted cables that were being analyzed, in parts, by over 50 media and human rights organizations from around the world.

For the past month WikiLeaks has been in the unenviable position of not being able to comment on what has happened, since to do so would be to draw attention to the decryption passwords in the Guardian book. Now that the connection has been made public by others we can explain what happened and what we intend to do.

More articles ...
- PayPal freezes WikiLeaks donations
- Statement on DDOS attacks
- Statement on Cablegate
- Nota à Imprensa
- Cables reveal history of secret cooperation between Swedish and US governments
- Editorial - 100 Days of Cablegate
- Media Currently Publishing
- WIKILEAKS PRESS RELEASE
- Wikileaks Statement on the 9 Month Anniversary of Cablegate: Release of 133,887 Cables
- 30 new revelations from #wlfind

WikiLeaks has commenced pre-litigation action against the Guardian and an individual in Germany who was distributing the Guardian passwords for personal gain.

Over the past nine months, WikiLeaks has been releasing US diplomatic cables according to a carefully laid out plan to stimulate profound changes. A number of human rights groups, including Amnesty International, believe that the co-ordinated release of the cables contributed to triggering the Arab Spring. By forming partnerships with over 90 other media and human rights organizations WikiLeaks has been laying the ground for positive political change all over the world.

The WikiLeaks method involves a sophisticated procedure of packaging leaked US diplomatic cables up into country groups or themes, such as 'resources corruption', and providing it to those organizations that agreed to do the most research in exchange for time-limited exclusivity. As part of the WikiLeaks agreement, these groups, using their local knowledge, remove the names of persons reporting unjust acts to US embassies, and feed the results back to WikiLeaks. WikiLeaks then publishes, simultaneously with its partners, the underlying cables together with the politically explosive revelations. This way publications that are too frightened to publish the cables have the proof they need, and the public can check to make sure the claims are accurate.

Over time WikiLeaks has been building up, and publishing, the complete Cablegate "library"—the most significant political document ever published. The mammoth task of reading and lightly redacting what amounts to 3,000 volumes or 284 million words of global political history is shared by WikiLeaks and its partners. That careful work has been compromised as a result of the recklessness of the Guardian.

Revolutions and reforms are in danger of being lost as the unpublished cables spread to intelligence contractors and governments before the public. The Arab Spring would not have started in the manner it did if the Tunisian government of Ben Ali had copies of those WikiLeaks releases which helped to take down his government. Similarly, it is possible that the torturing Egyptian internal security chief, Suleiman—Washington's proposed replacement for Mubarak—would now be the acting ruler of Egypt, had he acquired copies of the cables that exposed his methods prior to their publication.

Indeed, it is one of the indelible stains on Hillary Clinton that she personally set course to forewarn dozens of corrupt leaders, including Hosni Mubarak, about some of the most powerful details of WikiLeaks' revelations to come.

Every day that the corrupt leadership of a country or organization knows of a pending WikiLeaks disclosure is a day spent planning how to crush revolution and reform.

Guardian investigations editor, David Leigh, recklessly, and without gaining our approval, knowingly disclosed the decryption passwords in a book published by the Guardian. Leigh states the book was rushed forward to be written in three weeks—the rights were then sold to Hollywood.

The following extract is from the Guardian book:

> *Leigh tried his best not to fall out with this Australian impresario, who was prone to criticise what he called the "snaky Brits". Instead, Leigh used his ever-shifting demands as a negotiating lever. "You want us to postpone the Iraq logs' publication so you can get some TV," he said. [WikiLeaks: We required more time for redactions and to complete three Iraq war documentaries commissioned through the Bureau of Investigative Journalism. The documentaries were syndicated through Channel 4 (UK) and al Jazeera English and Arabic] "We could refuse, and simply go ahead with publication as planned. If you want us to do something for you, then you've got to do something for us as well." He asked Assange to stop procrastinating, and hand over the biggest trove of all: the cables. Assange said, "I could give you half of them, covering the first 50% of the period."*

> *Leigh refused. All or nothing, he said. "What happens if you end up in an orange jump-suit en route to Guantánamo before you can release the full files?"* ***In return he would give Assange a promise to keep the cables secure****, and not to publish them until the time came. Assange had always been vague about timing: he generally indicated, however, that October would be a suitable date. He believed the US army's charges against the imprisoned soldier Bradley Manning would have crystallised by then, and publication could not make his fate any worse. He also said, echoing Leigh's gallows humour: "I'm going to need to be safe in Cuba first!" Eventually, Assange capitulated. Late at night, after a two-hour debate, he started the process on one of his little netbooks that would enable Leigh to download the entire tranche of cables. The Guardian journalist had to set up the PGP encryption system on his laptop at home across the other side of London. Then he could feed in a password. Assange wrote down on a scrap of paper:*

> *[WikiLeaks: we have replaced the password with Xs]*
> *XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX*

> *"That's the password," he said. "But you have to add one extra word when you type it in. You have to put in the word 'XXXXXXX' before the word 'XXXXXX' [WikiLeaks: so if the paper were seized, the password would not work without Leigh's co-operation] Can you remember that?" "I can remember that." Leigh set off home, and successfully installed the PGP software.*

The Guardian disclosure is a violation of the confidentiality agreement between WikiLeaks and Alan Rusbridger, editor-in-chief of the Guardian, signed July 30, 2010. David Leigh is also Alan Rusbridger's brother in law, which has caused other Guardian journalists to claim that David Leigh has been unfairly protected from the fallout. It is not the first time the WikiLeaks security agreement has been violated by the Guardian.

WikiLeaks severed future projects with the Guardian in December last year after it was discovered that the Guardian was engaged in a conspiracy to publish the cables without the knowledge of WikiLeaks, seriously compromising the security of our people in the United States and an alleged source who was in pre-trial detention. Leigh, without any basis, and in a flagrant violation of journalistic ethics, named Bradley Manning as the Cablegate source in his book. David Leigh secretly passed the entire archive to Bill Keller of the New York Times, in September 2011, or before, knowingly destroying WikiLeaks plans to publish instead with the Washington Post & McClatchy.

David Leigh and the Guardian have subsequently and repeatedly violated WikiLeaks security conditions, including our requirements that the unpublished cables be kept safe from state intelligence services by keeping them only on computers not connected to the internet. Ian Katz, Deputy Editor of the Guardian admitted in December 2010 meeting that this condition was not being followed by the Guardian.

PJ Crowley, State Department spokesman on the cables issue earlier this year, told AP on the 30th of August, 2011 that "any autocratic security service worth its salt" would probably already have the complete unredacted archive.

Two weeks ago, when it was discovered that information about the Leigh book had spread so much that it was about to be published in the German weekly Freitag, WikiLeaks took emergency action, asking the editor not allude to the Leigh book, and tasked its lawyers to demand those maliciously spreading its details about the Leigh book stop.

WikiLeaks advanced its regular publication schedule, to get as much of the material as possible into the hands of journalists and human rights lawyers who need it. WikiLeaks and its partners were scheduled to have published most of the Cablegate material by November 29, 2011 – one year since the first publication. Over the past week, we have published over 130,000 cables, mostly unclassified. The cables have lead to hundreds of important news stories around the world. All were unclassified with the exception of the Australian, Swedish collections, and a few others, which were scheduled by our partners.

WikiLeaks has also been in contact with Human Rights Watch and Amnesty at a senior level. We contacted the US embassy in London and then the State Department in Washington on 25 August to see if their informant notification program, instituted last year, was complete, and if not, to take such steps as would be helpful. Only after repeated attempts through high level channels and 36 hours after our first contact, did the State Department, although it had been made aware of the issue, respond. Cliff Johnson (a legal advisor at the Department of State) spoke to Julian Assange for 75 minutes, but the State Department decided not to meet in person to receive further information, which could not, at that stage, be safely transmitted over the telephone.

ANEXO XXII: Artículo de *The Guardian* publicado el 2 de septiembre de 2011.

WikiLeaks

WikiLeaks publishes full cache of unredacted cables

Former media partners condemn WikiLeaks' decision to make public documents identifying activists and whistleblowers

James Ball

@jamesrbuk

Friday 2 September 2011 12.55 BST

WikiLeaks has published its full archive, including diplomatic cables marked by the US to indicate sources could be in danger. Photograph: Karen Bleier/AFP/Getty Images

WikiLeaks has published its full archive of 251,000 secret US diplomatic cables, without redactions, potentially exposing thousands of individuals named in the documents to detention, harm or putting their lives in danger.

The move has been strongly condemned by the five previous media partners – the Guardian, New York Times, El Pais, Der Spiegel and Le Monde – who have worked with WikiLeaks publishing carefully selected and redacted documents.

"We deplore the decision of WikiLeaks to publish the unredacted state department cables, which may put sources at risk," the organisations said in a joint statement.

"Our previous dealings with WikiLeaks were on the clear basis that we would only publish cables which had been subjected to a thorough joint editing and clearance process. We will continue to defend our previous collaborative publishing endeavour. We cannot defend the needless publication of the complete data – indeed, we are united in condemning it.

"The decision to publish by Julian Assange was his, and his alone."

Diplomats, governments, human rights charities and media organisations had urged WikiLeaks's founder, Assange, not to publish the full cache of cables without careful source protection.

The newly published archive contains more than 1,000 cables identifying individual activists; several thousand labelled with a tag used by the US to mark sources it believes could be placed in danger; and more than 150 specifically mentioning whistleblowers.

The cables also contain references to people persecuted by their governments, victims of sex offences, and locations of sensitive government installations and infrastructure.

WikiLeaks has published its full archive in an easily accessible and searchable manner, the first time the content has been made widely available to those without sophisticated technical skills.

It conducted a poll of its Twitter followers to decide whether to publish the documents, which it initially said was running at "100 to one" in favour of publishing. WikiLeaks did not disclose the final tallies, nor how many individuals responded to its poll.

Reporters Without Borders, a press freedom group which had been maintaining a backup version of the WikiLeaks site, revoked its support for the whistleblowing site in the wake of the decision.

"Some of the new cables have reportedly not been redacted and show the names of informants in various countries, including Israel, Jordan, Iran and Afghanistan," it said in a statement. "While it has not been demonstrated that lives have so far been put in danger by these revelations, the repercussions they could have for informants, such as dismissal, physical attacks and other reprisals, cannot be neglected."

The whistleblowing website began releasing the cables in December 2010, in conjunction with five media organisations including the Guardian. The mainstream news organisations carefully selected cables and before publication removed any information which could lead to sensitive sources being identified.

WikiLeaks claimed its disclosure was prompted after conflicts between Assange and former WikiLeaks associates led to one highlighting an error made months before. When passing the documents to the Guardian, Assange created a temporary web server and placed an encrypted file containing the documents on it. The Guardian was led to believe this was a temporary file and the server would be taken offline after a period of hours.

However, former WikiLeaks staff member Daniel Domscheit-Berg, who parted acrimoniously with WikiLeaks, said instead of following standard security precautions and creating a temporary folder, Assange instead re-used WikiLeaks's "master password". This password was then unwittingly placed in the Guardian's book on the embassy cables, which was published in February 2011.

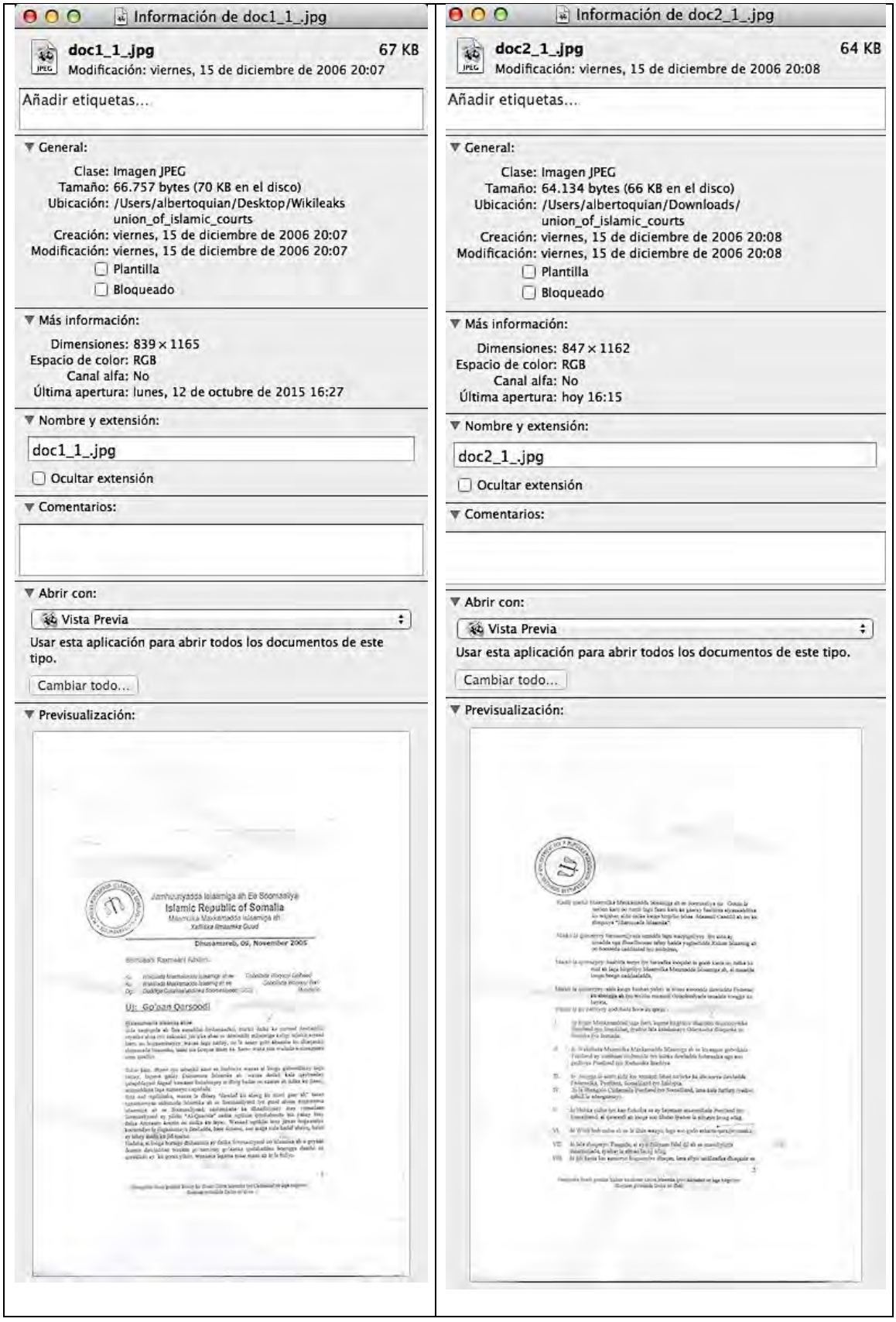
Separately, a WikiLeaks activist had placed the encrypted files on BitTorrent, a peer-to-peer file sharing network, in the hours before Julian Assange was imprisoned pending extradition proceedings in December 2010, as a form of insurance for the site. Fewer than five people knew of the existence of the site.

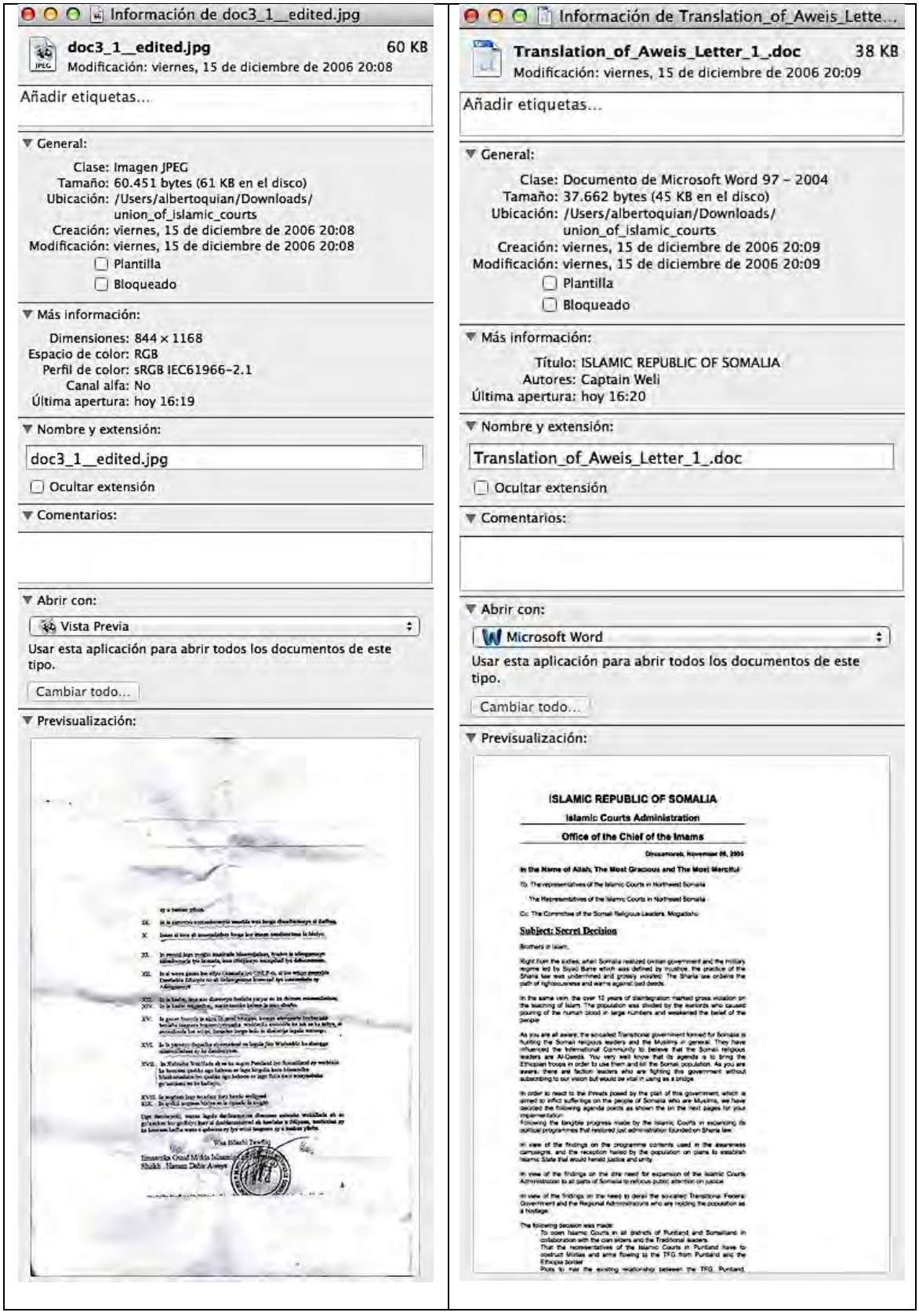
As former activists' disillusionment with WikiLeaks grew, one told German magazine Freitag about the link between the publicly available password and files in an attempt to highlight sloppy security at WikiLeaks. The magazine published the story with no information to identify the password or files.

WikiLeaks then published a series of increasingly detailed tweets giving clues about where the password might be found as part of its attempts to deny security failings on its own part. These are believed to have led a small group of internet users to find the files, which were published in a difficult-to-access format requiring significant technical skill, on rival leak site Cryptome.

Domscheit-Berg, often referred to as Assange's former deputy at WikiLeaks, condemned the password reuse. "The file was never supposed to be shared with anyone at all," he said. "To get a copy you would usually make a new copy with a new password. He [Assange] was too lazy to create something new."

ANEXO XXIII: Metadatos del primer documento secreto publicado por WikiLeaks.




Información de doc3_1__edited.jpg
doc3_1__edited.jpg
60 KB
Modificación: viernes, 15 de diciembre de 2006 20:08
Añadir etiquetas...
General:
Clase: Imagen JPEG
Tamaño: 60.451 bytes (61 KB en el disco)
Ubicación: /Users/albertoquian/Downloads/union_of_islamic_courts
Creación: viernes, 15 de diciembre de 2006 20:08
Modificación: viernes, 15 de diciembre de 2006 20:08
Plantilla
Bloqueado
Más información:
Dimensiones: 844 × 1168
Espacio de color: RGB
Perfil de color: sRGB IEC61966-2.1
Canal alfa: No
Última apertura: hoy 16:19
Nombre y extensión:
doc3_1__edited.jpg
Ocultar extensión
Comentarios:
Abrir con:
Vista Previa
Usar esta aplicación para abrir todos los documentos de este tipo.
Cambiar todo...
Previsualización:
Información de Translation_of_Aweis_Lette...
Translation_of_Aweis_Letter_1_.doc
38 KB
Modificación: viernes, 15 de diciembre de 2006 20:09
Añadir etiquetas...
General:
Clase: Documento de Microsoft Word 97 - 2004
Tamaño: 37.662 bytes (45 KB en el disco)
Ubicación: /Users/albertoquian/Downloads/union_of_islamic_courts
Creación: viernes, 15 de diciembre de 2006 20:09
Modificación: viernes, 15 de diciembre de 2006 20:09
Plantilla
Bloqueado
Más información:
Título: ISLAMIC REPUBLIC OF SOMALIA
Autores: Captain Weli
Última apertura: hoy 16:20
Nombre y extensión:
Translation_of_Aweis_Letter_1_.doc
Ocultar extensión
Comentarios:
Abrir con:
Microsoft Word
Usar esta aplicación para abrir todos los documentos de este tipo.
Cambiar todo...
Previsualización:
ISLAMIC REPUBLIC OF SOMALIA
Islamic Courts Administration
Office of the Chief of the Imams
In the Name of Allah, The Most Gracious and The Most Merciful
Subject: Secret Decision